



Operations, Safety & Security (OSS) Committee Meeting

Thursday, August 21, 2025 at 3:00 PM

In Person & Videoconference - Administration Building - 1100 Cherry Street - Freeport

This meeting agenda with the agenda packet is posted online at www.portfreeport.com

The meeting will be conducted pursuant to Section 551.127 of the Texas Government Code titled "Videoconference Call." A quorum of the OSS Committee, including the presiding officer, will be present at the Commissioner Meeting Room located at 1100 Cherry Street, Freeport, Texas. The public will be permitted to attend the meeting in person or by videoconference.

Join Zoom Meeting

<https://us02web.zoom.us/j/86212016933?pwd=aNSq8VeGtdhrar9pBaTGaY1jTlwd5z.1>

Meeting ID: 862 1201 6933

Passcode: 790817

- 1. Committee Members: Santos (Chairman), Croft, Kincannon**
- 2. CONVENE OPEN SESSION in accordance with Texas Government Code Section 551.001, et. seq., to review and consider the following:**
- 3. Roll Call.**
- 4. Public Comment.**

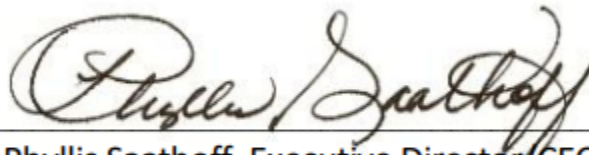
Public comment on any matter not on this Agenda will be limited to 5 minutes per participant and can be completed in person or by video conference.
- 5. Public Testimony.**

Public testimony on any item on this Agenda will be limited to 5 minutes per agenda item to be addressed per participant and can be completed in person or by videoconference. The participant shall identify in advance the specific agenda item or items to be addressed.
- 6. Receive demo for Video Analytics.**
- 7. Discussion regarding proposals received for Video Analytics.**

8. **Receive update from Riviana regarding TWIC violations and mitigation actions.**
9. **Review of proposals received for Camera Replacement project.**
10. **EXECUTIVE SESSION in accordance with Subchapter D of the Open Meetings Act, Texas Government Code Section 551.001, et. seq., to review and consider the following:**
 - A. Under authority of Section 551.076 (Deliberation of Security Matters):
 1. Discussion regarding issues related to the deployment, or specific occasions for implementation of security personnel or devices or security audit and services.
11. **RECONVENE OPEN SESSION:**
12. **Adjourn.**

The Committee does not anticipate going into a closed session under Chapter 551 of the Texas Government Code at this meeting for any other items on the agenda, however, if necessary, the Committee may go into a closed session as permitted by law regarding any item on the agenda.

With this posted notice, Port Commissioners have been provided certain background information on the above listed agenda items. Copies of this information can be obtained by the public at the Port Administrative offices at 1100 Cherry Street, Freeport, TX.



Phyllis Saathoff, Executive Director/CEO
PORT FREEPORT

Participation is welcomed without regard to race, color, religion, sex, age, national origin, disability or family status. In accordance with Title II of the Americans with Disabilities Act and Section 504 of the Rehabilitation Act, persons with disabilities needing reasonable accommodations to participate in this proceeding, or those requiring language assistance (free of charge) should contact the Executive Assistant no later than forty-eight (48) hours prior to the meeting, at (979) 233-2667, ext. 4326, email: bevers@portfreeport.com.

La participación es bienvenida sin distinción de raza, color, religión, sexo, edad, origen nacional, discapacidad o situación familiar. De acuerdo con el Título II de la Ley de Estadounidenses con Discapacidades y la Sección 504 de la Ley de Rehabilitación, las personas con discapacidades que necesiten adaptaciones razonables para participar en este procedimiento, o aquellas que requieran asistencia lingüística (sin cargo), deben comunicarse con el Asistente Ejecutivo a más tardar cuarenta -ocho (48) horas antes de la reunión, al (979) 233-2667, ext. 4326, correo electrónico: bevers@portfreeport.com.



DIGI
SECURITY SYSTEMS

We have prepared a quote for you

**Port Freeport - RFP Proposal for Advanced
Video Analytics Solution - TIPS Contract
250101**

Quote # 019356
Version 1

Prepared for:

Port Freeport

Chris Hogan
hogan@portfreeport.com

Wednesday, July 16, 2025

Port Freeport
Chris Hogan
801 Navigation BLVD
Freeport, TX 77541
hogan@portfreeport.com

Dear Chris,

Digi Security Systems proposes BriefCam's advanced video analytics platform to meet the requirements outlined in the RFP for a Video Analytic Solution. Powered by artificial intelligence (AI) and deep learning, BriefCam delivers a comprehensive, on-premises solution that transforms live and recorded video into searchable, actionable, and quantifiable intelligence. This proposal demonstrates how BriefCam fulfills all required and preferred functionalities, integrates seamlessly with Milestone XProtect Smart Client 2023 R3 and AXIS cameras, supports 100 cameras (scalable to 200), and achieves over 95% accuracy. With centralized administration, redundant hardware, NIST-compliant facial recognition, and robust training and support, BriefCam ensures operational efficiency, scalability, and reliability.

BriefCam's Video Content Analytics platform leverages a convolutional neural network (CNN) architecture to provide high-accuracy object detection, classification, and analysis. The solution is optimized for scalability, efficiency, and seamless integration with the specified Milestone environment and AXIS cameras. Below, we detail how BriefCam meets the RFP's general requirements, compatibility specifications, required and preferred functionalities, and miscellaneous items.

General Requirements

- **AI and Deep Learning:** BriefCam's CNN-based architecture ensures advanced image processing and pattern recognition with >95% accuracy, delivering searchable, actionable, and quantifiable intelligence from live or recorded video.
- **Single Solution:** All required analytical functions (search, alert, intelligence) are provided within BriefCam's unified platform.
- **Centralized Administration:** A web-based interface allows centralized management of cameras, hosts, GPUs, and services, with scheduling for continuous, one-time, daily, or weekly video processing.
- **On-Premises Deployment:** BriefCam offers a fully on-premises solution with redundant power supplies and hardware to ensure uninterrupted operation and sufficient bandwidth. Continuous security monitoring detects malicious or unauthorized activity.
- **Scalability:** Supports 100 cameras with hardware expandable to 200, ensuring future-proofing.
- **Concurrent Users:** Supports a minimum of five concurrent users, with scalable user access.
- **Open Platform:** BriefCam's open architecture ensures compatibility with diverse VMS and camera models including Milestone XProtect and Axis cameras

Port Freeport Requirements:

- 10U of rack space in provided network rack
- Necessary power for all devices associated to this project.
- Provide sufficient open network switch ports for all devices requiring connection to the main network.
- Provide access to all areas necessary for completion of this project.

Compatibility

- **Operating Systems:** Compatible with Windows 10 and Windows 11.
- **VMS Integration:** Fully compatible with Milestone XProtect Smart Client 2023 R3 and newer.
- **Browsers:** Supports Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari on Mac and iPad.
- **Codecs:** Compatible with H.263, H.264, H.265, H.265/HEVC, and MPEG-4.
- **Cameras:** Compatible with AXIS cameras.
- **Video Formats:** Supports .264, .ASF, .AVI, .MOV, .MP3, .MP4, .WMV, and .RAW formats.

Intelligence Capabilities

BriefCam's intelligence module provides customizable dashboards for operational and business intelligence, including:

- Visualization of object movement, demographic segmentations, behavior trends, hotspots, and object interactions.
- Auto-generated charts and prioritized data points for actionable insights.
- Real-time alerts via email, text, or app based on object classification and recognition filters.

Warranty Coverage

Digi Security Systems and Briefcam provides a comprehensive warranty for the video analytics solution, fully compliant with the RFP requirements:

All Digi provided hardware (servers, cabling, and ancillary equipment) are warranted against defects in materials, workmanship, and performance for a minimum of one (1) year from the date of final commissioning and acceptance by Port Freeport.

The BriefCam 24/7 Support and Maintenance Package is fully included in this bid proposal, providing comprehensive support and ongoing maintenance for all associated systems and equipment for one (1) year.

Under the terms of this warranty, any defective hardware components will be promptly repaired or replaced with new, OEM-specification parts fully compatible with the installed system, at no cost to Port Freeport. This warranty coverage extends for a minimum of one (1) year from the date of final commissioning and acceptance by Port Freeport, with next-business-day service provided to ensure minimal disruption.

Response and Resolution Times

- **Critical Issues:** Guaranteed response time of 4–8 hours for issues affecting system functionality, with on-site support initiated within 24 hours of notification.
- **Non-Critical Issues:** Addressed within 2 business days of notification, with resolution completed within 5 business days. Additional time may be requested with Port Freeport's approval in case of supply chain delays.

Support and Documentation

- **Training:** Briefcam will provide a minimum of eight (8) hours of comprehensive training, including hands-on sessions and documentation, to ensure users are proficient in operating BriefCam's platform. Training will cover system setup, analytics configuration, and advanced features like search, alerts, and intelligence dashboards.
- **Support:** Briefcam 24/7 technical support and maintenance services are included, with guaranteed response times and regular software updates to maintain compatibility and performance.
- **Milestone Certifications:** Digi has two Milestone certified technicians that are the head of Digi's ERG group that will lead the implementation of this project.

Covered Components

- BriefCam will provide maintenance and support for all software applications and modules related to the solution for one (1) year
- Digi Security Systems will provide maintenance and support for analytics servers & storage appliances provided in this package for one (1) year - Upon request, Port Freeport will be provided with comprehensive options for extended support and maintenance services beyond the initial one-year warranty period, tailored to meet ongoing operational needs.

Preventive Maintenance

Digi will perform preventive maintenance, including:

- Full system health diagnostics
- Performance optimization reviews
- Hardware inspections per manufacturer guidelines
- Preventive maintenance scheduling will be coordinated with Port Freeport to avoid operational disruptions

Software Updates and Upgrades

We will ensure:

- Delivery and installation of all BriefCam and Milestone patches, updates, and firmware revisions
- Deployment testing in a secure, controlled environment to prevent service interruption
- All system licenses remain valid and covered under support agreements throughout the term

Corrective Maintenance

- All repair or replacement of faulty servers, or cabling will be provided at no additional cost during the contract period
- Replacement components will meet OEM specifications and system compatibility standards

Technical Support and Escalation

- Digi will assign a dedicated support manager for all maintenance and escalation needs
- Remote diagnostics and troubleshooting will be available with Digi's on-call support team
- On-site technician dispatch will be provided when required, with defined escalation tiers for after-hours issues
- Support availability will include both business hours and after-hours emergency response

Cybersecurity and Compliance

- All maintenance activities will comply with federal, state, and local regulations, as well as industry security standards
- Updates will address known vulnerabilities and align with cybersecurity best practices

Contract Term

- The initial term will extend through October 31, 2026

Pricing and Cost Transparency

- Fixed costs for quarterly preventive maintenance
- No-cost replacements under the contract period
- Clearly outlined hourly rates for any work outside of scope, including after-hours and emergency services

Insurance and Liability

- Digi maintains comprehensive insurance coverage, including:
 - General Liability

Implementation Plan:

1. Assessment and Planning: Starting September 1st

- Conduct site survey and assess existing Milestone and AXIS camera infrastructure.
- Finalize hardware specifications for 100 cameras (scalable to 200).

2. Hardware and Software Deployment: Starting September 14th

- Install on-premises servers with redundant power supplies and security monitoring.
- Deploy BriefCam software and integrate with Milestone XProtect.

3. Configuration and Testing: Starting September 22nd

- Configure analytics, search, alert, and intelligence functions.
- Perform system testing to ensure >95% accuracy and compatibility.

4. Training and Handover: Starting September 29th

- Deliver 8+ hours of training for up to five concurrent users.
- Provide user manuals and ongoing support documentation.

Digi Security Systems Current Clients Include:

Digi Security Systems is proud to serve a diverse range of government, educational, and public sector organizations across Texas, Oklahoma, and Arkansas. Below is a list of current clients and cooperative purchasing partners relevant to the RFP for the Video Analytic Solution, demonstrating our experience and reliability in delivering tailored security solutions.

• Tinker Air Force Base

- Digi Security Systems provides advanced security solutions, including access control and surveillance systems, to support the operational and safety needs of Tinker Air Force Base in Oklahoma.

• Houston Police Department

- Digi partners with the Houston Police Department to deliver integrated security systems, enhancing public safety through cutting-edge technology deployments in the Houston metropolitan area.

• Dallas Independent School District (Dallas ISD)

- Digi serves Dallas ISD, supporting over 144,000 students and 21,000 staff across 241 schools with customized

security solutions, including video surveillance and access control systems. Recent projects include district-wide server refreshes with expanded storage and new warranties.

- **Fort Worth Independent School District (Fort Worth ISD)**

- Digi provides comprehensive security systems to Fort Worth ISD, ensuring the safety of students, staff, and facilities through tailored electronic and digital security solutions.

- **Oklahoma City Public Schools (OKC Public Schools)**

- Digi is a trusted provider for OKC Public Schools, delivering security solutions to protect educational environments.

- **University of Oklahoma**

- Digi supports higher education security needs at the University of Oklahoma with advanced surveillance and access control systems.

- **Oklahoma State Agencies**

- Through Oklahoma Management and Enterprise Services (OMES), Digi is a preferred vendor for state agencies, providing security solutions under state contract pricing.

- **Oklahoma Municipalities**

- Digi is the top choice for Oklahoma municipalities, offering jail control systems and other security solutions through cooperative contracts.

Why Choose Digi Security Systems and BriefCam?

- **Proven Expertise:** Digi Security Systems has extensive experience deploying video analytics solutions, with certified BriefCam technicians.
- **Industry-Leading Solution:** BriefCam is a globally recognized leader in video analytics, delivering unmatched accuracy and flexibility.
- **Compliance and Reliability:** NIST-compliant facial recognition, redundant hardware, and continuous security monitoring ensure trust and uptime.
- **Scalability and Future-Proofing:** Supports growth to 200 cameras and evolving surveillance needs.

Digi Security Systems is committed to delivering a state-of-the-art video analytics solution that meets your operational and security needs. We look forward to partnering with you to implement BriefCam's industry-leading platform.

11333 East 51st Place
Tulsa, OK 74146
www.digiss.com
(918) 824-2520



DIGI
SECURITY SYSTEMS

Sean Hardani
Account Manager
Digi Security Systems - Tulsa

Briefcam Video Analytics Software

Description		Qty
IS-BAS-001	BriefCam Insights Base Package - (Number of Concurrent Users - 5 - Number of RESEARCH Users - 5 - (1 x Editor; 4 x Viewer)Number of Cameras - 100Number of RESPOND)	1
IS-RSP-001	RESPOND Pack Insights (1-99 cameras) - Price per 1 Additional Real-Time Camera Stream	90
IS-MNT-001	Insights Software SCC - 1st Year - (Standard Customer Care Program Includes: - Upgrade to latest BriefCam release versions and updates- Technical Support in accordance with BriefCam SLA- Self-Help Support - access to Online Training Courses (LMS)- 24x7	1
BC-RSR-BAS	Implementation Pack - Remote Distributed - Basic Deployment for 2-6 Servers	1
BC-TRN-005	Instructor Led Online End-User training - Per Day - Online	1

Subtotal: \$151,250.00

Briefcam Video Analytics Equipment

Description		Qty
BC-D-2-5415-000-256-19	VS Server - Dell R760XL2 x 480GB M2 SSD (OS in RAID1)8TB 7200RPM - 2 X Intel® Xeon® Gold 5415+ Processor 8C/2.90GHz 256GB RAM - 2x10GbE BASE-T + LOM 2x 10/25GbE SFP28 - 2 X 1400W Redundant Power SupplyWindows Server 2019 IoTIDRAC 9 ENT5 Years Dell Pr	1
BC-D-2-5415-1L4-128-19	Processing Server - (Dell R760XL2 x 480GB M2 SSD (OS in RAID1)8TB 7200RPM - 2 X Intel® Xeon® Gold 5415+ Processor 8C/2.90 GHz 128GB RAM Nvidia L4 24GB - 2x10GbE BASE-T + LOM 2x 10/25GbE SFP28 2 X 1400W Redundant Power Supply Windows Server 2019 IoT IDRAC	1
BCD-D-2-6542Y-3L4-256-LX	OX6 Alert Processing Server - Dell R760XL2 x 480GB M2 SSD (OS in RAID1)2 x Intel® Xeon® Gold 6542Y Processor 24C/2.90 GHz256GB RAM3 X Nvidia L4 24GB 2x10GbE BASE-T + LOM 2x 10/25GbE SFP282 X 1400W Redundant Power SupplyUbuntu Server 22.04.2IDRAC 9	2
BCD-D-1-E2486-000-64-19	Database Server - Dell R3602 x 480GB M2 SSD (OS in RAID1)Intel® Xeon® E-2486 Processor 18M Cache, 3.50 GHz64GB RAM2x1GbE RJ45, 2x10GbE RJ452 X 600W Redundant Power SupplyWindows Server 2019 IoTIDRAC 9 ENT5 Years Dell Pro-Support	1
Shipping	Shipping/Processing	1

Subtotal: \$109,042.50

11333 East 51st Place
Tulsa, OK 74146
www.digiss.com
(918) 824-2520



DIGI
SECURITY SYSTEMS

Installation of Briefcam Video Analytics Software & Equipment

Product Details

SENIOR TECH

Certified Senior Technician Labor Hours (Onsite Hardware Install + Integration & Support Testing)

Subtotal: \$11,200.00

Digi Onsite Service Plan for Briefcam Server Hardware

Product Details

1 YEAR Onsite Service Plan

Digi Onsite Service Plan for Briefcam Server Hardware

Subtotal: \$6,500.00

Port Freeport - RFP Proposal for Advanced Video Analytics Solution - TIPS Contract 250101



Prepared by:

Digi Security Systems - Tulsa

Sean Hardani
(918) 824-0001
seanh@digiss.com

Prepared for:

Port Freeport

801 Navigation BLVD
Freeport, TX 77541
Chris Hogan
(979) 481-1285
hogan@portfreeport.com

Quote Information:

Quote #: 019356

Version: 1
Delivery Date: 07/16/2025
Expiration Date: 08/07/2025

Quote Summary

Description	Amount
Briefcam Video Analytics Software	\$151,250.00
Briefcam Video Analytics Equipment	\$109,042.50
Installation of Briefcam Video Analytics Software & Equipment	\$11,200.00
Digi Onsite Service Plan for Briefcam Server Hardware	\$6,500.00

Total: \$277,992.50

This quotation does not include applicable taxes unless specifically listed above. Acceptance of this quote or any purchase order generated as a result of this quote indicates acceptance of the Digi standard terms and conditions. The Digi standard terms and conditions can be found at www.digiss.com or a copy may be requested from your Digi representative. Upon approval, a 30% mobilization deposit, excluding taxes, is due immediately. The remaining 70% will be billed based upon monthly billing milestones or substantial completion of the project. All applicable taxes will be billed upon substantial completion of the project. Exceptions to this policy are possible and include adherence to internal customer purchasing policy, governing AIA billing schedules, or other agreements in writing between the approving customer and Digi. For clarifications, questions, or edits to this policy please contact your Digi representative. This proposal is valid for 30 days. Conduit, back boxes, and hangers are excluded from this proposal unless specifically listed above. All 120v work is excluded from this proposal unless specifically listed. All painting and patching is excluded. Asbestos work of any kind is excluded from this proposal. No cost for any required abatement is included in this proposal. Any materials, work, or equipment not explicitly listed in this proposal is excluded. Any cancellation or returns are subject to a restocking fee and other charges, for which the Purchaser shall be responsible.

Digi Security Systems - Tulsa

Port Freeport

Signature: 

Name: Sean Hardani

Title: Account Manager

Date: 07/16/2025

Signature: _____

Name: Chris Hogan

Date: _____



CERTIFICATE OF LIABILITY INSURANCE

12/15/2025

DATE (MM/DD/YYYY)

7/15/2025

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Lockton Companies, LLC DBA Lockton Insurance Brokers, LLC in CA CA license #0F15767 1185 Avenue of the Americas, Ste. 2010 New York NY 10036 (646) 572-7300	CONTACT NAME:	FAX (A/C, No):	
	PHONE (A/C, No, Ext):	E-MAIL ADDRESS:	
INSURED 1552693 Digi Security Systems, LLC 11333 E. 51st Pl. Tulsa OK 74146	INSURER(S) AFFORDING COVERAGE		NAIC #
	INSURER A: Chubb Indemnity Insurance Company		12777
	INSURER B: Great Northern Insurance Company		20303
	INSURER C: Chubb National Insurance Company		10052
	INSURER D: Chubb National Insurance Company		10052
	INSURER E:		
INSURER F:			

COVERAGES **CERTIFICATE NUMBER:** 22169748 **REVISION NUMBER:** XXXXXXXX

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input checked="" type="checkbox"/> PRO-JECT <input checked="" type="checkbox"/> LOC OTHER:	N	N	D02775189	12/15/2024	12/15/2025	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000 MED EXP (Any one person) \$ 15,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ 2,000,000 \$
B	<input checked="" type="checkbox"/> AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS ONLY <input checked="" type="checkbox"/> NON-OWNED AUTOS ONLY	N	N	73647367	12/15/2024	12/15/2025	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ XXXXXXXX BODILY INJURY (Per accident) \$ XXXXXXXX PROPERTY DAMAGE (Per accident) \$ XXXXXXXX Reten/Deduc \$ 1,000
C	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED <input checked="" type="checkbox"/> RETENTION \$ 10,000	N	N	56725896	12/15/2024	12/15/2025	EACH OCCURRENCE \$ 6,000,000 AGGREGATE \$ 6,000,000 \$ XXXXXXXX
D	<input checked="" type="checkbox"/> WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	<input checked="" type="checkbox"/> Y <input checked="" type="checkbox"/> N	N	71835725	12/15/2024	12/15/2025	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER

22169748
Port Freeport
Chris Hogan
801 Navigation Blvd
Freeport TX 77541

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

© 1988-2015 ACORD CORPORATION. All rights reserved.



BRIEFCAM PLATFORM

DATASHEET

 BriefCam

The BriefCam® comprehensive Video Content Analytics platform empowers people, companies, and communities of any size to realize the value of their video surveillance content by making video searchable, actionable, and quantifiable. Review hours of video in minutes; respond immediately to critical situational changes in the environment; and quantitatively analyze video to derive actionable insights for data-driven safety, security and operational decision making, all while effectively balancing sensitivity, accuracy, and efficiency:

INNOVATIVE & EXTENSIBLE PLATFORM: A robust portfolio of critical video analytics capabilities fully integrated across the platform for video metadata search, alerting, and visualization, powerfully extending the value of video surveillance investments. BriefCam supports integrations with an ever-expanding set of leading Video Management Systems (VMS) driving best-of-breed video solutions for heightened user experiences.

UNMATCHED ACCURACY: Market leading accuracy for detection and classification across object classes, attributes, behaviors, as well as appearance similarity and face and license plate recognition.

SUPERIOR PERFORMANCE: Effectively supports the requirement for both on-demand and real-time analytics for full camera coverage and introduces AI-industry standard, Linux-based processing for increased real-time performance, precision, and speed.

CENTRALIZED ANALYTICS & ALERTS: With the BriefCam Nexus, multi-site customers can centrally view and analyze alerts generated at remote sites as well as business intelligence dashboard visualizations from all sites.

ELEVATED CUSTOMER EXPERIENCE: Dedicated consultancy, implementation, and support to ensure customers enjoy the quickest time to value, lowest total cost of ownership, and impactful analytics applications to maximize the investment in video.

BRIEFCAM SOLUTIONS



REVIEW

Accelerate Investigations

By leveraging REVIEW, users can pinpoint objects and events of interest to advance investigations and powerfully accelerate time to target. This solution supports effective case management, so investigators can organize video assets, bookmark objects of interest, summarize case findings, and export reports, while dynamically collaborating on cases with other users.

With REVIEW, operators can review hours of video in minutes and refine search results through filter tolerance as well as density, speed, direction, and sort controls. REVIEW enables:

- Maps visualization and comprehensive cross-camera search and filtering capabilities for enhanced investigations and case management.
- Visual layers, which presents activity, dwell time, common paths, and background changes as easily readable heatmaps for increased scene understanding.
- The patented BriefCam VIDEO SYNOPSIS® solution, which simultaneously presents objects that have appeared at different times within the video, resulting in a dramatically shorter video segment that fully preserves the viewer's ability to analyze the scene.



Train custom classes for video search, alerting & data visualization



Enrich investigations and case management with Maps visualization



RESPOND

Attain Situational Awareness

With BriefCam RESPOND you can trigger real-time alerts based on complex object classification and recognition filter combinations to increase situational awareness and deliver critical, time-sensitive intelligence. RESPOND empowers you to react to events as they unfold, from proactively protecting people and property to driving better visitor or customer engagement.

BriefCam allows for improved responsiveness, real-time decision-making, and effective balancing of sensitivity, accuracy, and efficiency with alerting rule configuration, face and license plate watchlist management, and alert notifications for messaging services and VMS alarm areas. BriefCam supports integrations with many VMS vendors including Genetec Security Center, Milestone XProtect, Axis ACS, Lenel OnGuard, Hanwha Wisenet WAVE, IndigoVision Control Center, Pelco VideoXPert, and more.



RESEARCH

Derive Operational & Business Intelligence

Uncover patterns, drive strategic decision-making, and optimize operational and business practices by aggregating video data in a fully-integrated, highly customizable business intelligence platform. BriefCam RESEARCH visualizes object movement, demographic segmentations, behavior trending, hotspots, and object interactions. It offers interactive, intuitive, and easy to use dashboards for data analysis, as well as tools for auto-generating and prioritizing relevant data points and charts.

With business intelligence, you can seamlessly correlate video analytics with third party data sources, such as Point of Sale, Time Management, and Access Control, for a uniquely informative view of your environment and export data to external business intelligence databases for further analysis and correlation.



DEVELOPER TOOLS

Better Together

UNIFIED OPEN API: Enables developers to deepen the integration between third-party applications and BriefCam.

RESPOND OUTBOUND API: Enables integration of BriefCam alerts into third-party alerting infrastructures.

SYSTEMS EVENT API: Enables a system event to be sent to any third-party system.



ADMINISTRATION

Ease of Use

CENTRALIZED ADMINISTRATION: View and activate cameras, configure hosts, GPUs, and services from a single web interface.

FLEXIBLE SCHEDULING: Schedule continuous, one-time, daily or weekly automatic video processing for each VMS video source, across all three platform modules.

SSO COMPATIBILITY: Support for secure third-party single sign-on authentication.

GDPR COMPLIANCE: Easily delete or export personally identifiable data, enabling GDPR compliance.

CROSS-PLATFORM VIDEO ANALYTIC CAPABILITIES

FEATURE	REVIEW Search	RESPOND Alert	RESEARCH Quantify
SOURCE Based on specific cameras or files	✓	✓	✓
TIME RANGE Based on specific time ranges	✓	✓	✓
CLASS Based on People (Man, Woman, Child), Two-Wheeled Vehicles (Bicycles, Motorcycles), Other Vehicles (Car, Pickup, Van, Truck, Bus, Train, Airplane, Boat), Illumination Changes, and Animals.	✓	✓	✓
CUSTOM CLASSIFIED Define, train on-site, and leverage custom classes for uniformed workers and 4-wheel vehicles. Available only with the Linux-based engine.	✓	✓	✓
PERSON ATTRIBUTES Based on person characteristics, including Lower and Upper Wear (by color), Hats, Face Masks, and Bags.	✓	✓	✓
COLOR Based on any combination of object color, including Brown, Red, Orange, Yellow, Green, Lime, Cyan, Blue, Purple, Pink, White, Grey, and Black	✓	✓	✓
VIDEO SYNOPSIS Simultaneously view objects that have appeared at different times in a video, or from smart alerts for accelerated video review	✓	✓	
FAST TRACK Quickly find objects across surrounding cameras based on geolocations defined in the integrated VMS.	✓		
CASE MANAGEMENT Organize all video assets of an investigation in a single container, bookmark objects of interest, and export case findings reports to support collaboration	✓		
APPEARANCE SIMILARITY Identify people and vehicles with similar attributes	✓		

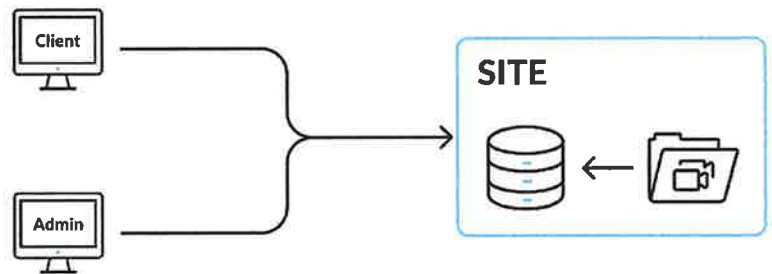
FEATURE	REVIEW Search	RESPOND Alert	RESEARCH Quantify
FACE RECOGNITION Based on images extracted from existing video or photo uploads, conduct “in the wild” face matching for persons included or excluded on watchlists. BriefCam offers versions with Face Recognition completely deactivated and excluded from the user interface.	✓	✓	✓
LICENSE PLATE RECOGNITION For in “in the wild” surveillance scenarios, recognize license plates based on watchlists for vehicle behavior analysis and traffic optimization	✓	✓	✓
VEHICLE MAKE AND MODEL RECOGNITION Identify vehicles by brand and type.	✓	✓	✓
PROXIMITY IDENTIFICATION Detect the distance between individuals over time and location for measuring compliance with physical distancing mandates, enabling contact tracing, and advancing investigations	✓	✓	✓
FACE MASK DETECTION Detect and identify face mask wearing and lack thereof for measuring compliance with public health mandates and safety codes	✓	✓	✓
PEOPLE COUNTING Count the number of people in a pre-defined area or who travelled in a certain direction, track queues and crowd formations, and measure occupancy to optimize space utilization and pedestrian traffic flows	✓	✓	✓
CROWD COUNTING Count the number of people in sizable crowds or areas, taking over from the People Counting algorithm for groups exceeding 50 people. Measure maximum and minimum crowd sizes over a set period of time. Available only with the Linux-based engine		✓	✓
AIRPLANE COUNTING Monitor the increase or decrease of airplanes in a pre-defined range of view or area. Available only with the Linux-based engine		✓	✓
GROUP DETECTION Receive alerts when a group of a pre-defined number forms in a certain area for a certain amount of time. Available only with the Linux-based engine		✓	
VISUAL LAYERS Create visual analytics and derive insights about activity, dwell time, common paths, and background changes	✓		✓
DIRECTION Based on the direction detected in the video	✓	✓	✓
SIZE Based on object’s actual calculated size	✓	✓	✓
PATH Identify objects traveling along one or more user-defined paths	✓	✓	✓
AREA Identify objects included or excluded within one or more user-defined 3- or 4-sided polygon areas	✓	✓	✓
SPEED Based on object’s actual calculated speed	✓	✓	✓
DWELL Based on object dwelling for pre-set time periods within a scene	✓	✓	✓
LINE CROSSING Detect demarcation crossings in a predefined direction	✓	✓	✓

PLATFORM EDITIONS			
PRODUCT	PROTECT	INSIGHTS	INVESTIGATOR
VIDEO INGESTION	File and VMS-based	VMS-based	File-based
PLATFORM MODULES	REVIEW, RESPOND, RESEARCH	REVIEW, RESPOND, RESEARCH	REVIEW
USERS	Multi-user	Multi-user	Single User Multi-user (Investigator for Teams)
INFRASTRUCTURE	OX5 Windows-based or OX6 Linux-based	OX5 Windows-based or OX6 Linux-based	OX5 Windows-based

PLATFORM ARCHITECTURES

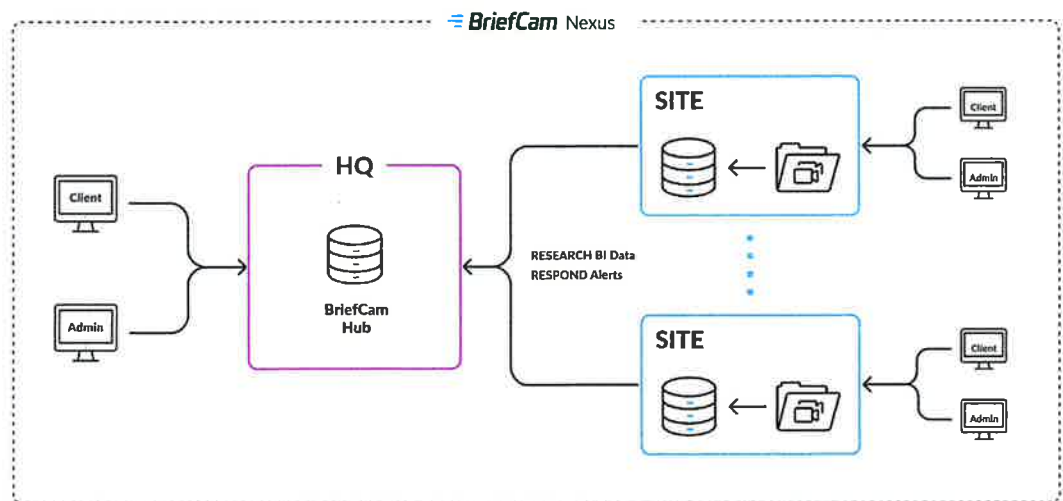
STANDALONE ARCHITECTURE

A BriefCam system for facilities of any size that includes REVIEW, RESPOND and RESEARCH. Internal architecture may include a Linux-based engine for customers to maximize real-time performance and accuracy, while reducing the total cost of system ownership.



MULTI-SITE ARCHITECTURE

To learn more about our multi-site architecture please visit our BriefCam Nexus datasheet.



TECHNICAL SPECIFICATIONS

RECOMMENDED VIDEO STREAM RESOLUTION	Minimum CIF (352 x 240), Maximum 4K (3840 X 2160)
RECOMMENDED FRAME RATE (FPS)	8-30 frames per second
SUPPORTED VIDEO FILE FORMATS	.264, .3GP, .ASF, .AVI, .DAV, .DIVX, .DVR*, .FLV, .G64, .G64X, .GE5, .MKV, .MOV, .MP4, .RAW, .RT4, .TS, .WMV, .XBA (single & multi-stream)
SUPPORTED CODECS	H.264, H.265/HEVC, MPEG-4, H.263 (H.265 is supported for selected VMSs and cameras)
FILE-BASED INGESTION	Multi-file videos or single file videos
SUPPORTED VMS PLATFORMS	American Dynamics, Arcanes Technology, Avigilon, Axis, Bosch, CASD, Dallmeier, Digifort, Digital Watchdog, Exacq, FLIR, Genetec, Geutebruck, Hanwha, Hikvision, IndigoVision, Intellicene, IPConfigure, ISS, LenelS2, March Networks, Milestone, Network Optix, Panasonic i-PRO, Pelco, Qognify, Salient, Surveillus*, Synectics*, Teleste, Verint * Plugins created by the VMS partner
SUPPORTED CAMERA TYPES	Fixed Cameras
SINGLE SIGN-ON (SSO)	Microsoft Active Directory, both LDAP and LDAPS, including user groups (OU support), and the SAML protocol
FACE RECOGNITION	Minimum Face Size: 40x40 pixels across the person's face, 20 pixels between the eyes, or 400 pixels per meter
SUPPORTED LANGUAGES	Arabic, Brazilian Portuguese, Bulgarian (not including RESEARCH), Chinese Simplified, Chinese Traditional, Danish, Dutch, English, Finnish, French, German, Hebrew, Italian, Japanese, Korean, Latin Spanish, Russian, Thai, Turkish, Ukrainian, Vietnamese
SUPPORTED BROWSERS	Google Chrome Desktop and Microsoft Edge (not supported in BriefCam Nexus)

ABOUT BRIEFCAM

BriefCam® is the leading provider of video analytics software that enables people, companies, and communities to unlock the value of video surveillance content. Delivering accurate, flexible, and comprehensive solutions, BriefCam's video analytics platform provides valuable insights for accelerating investigations, increasing situational awareness, and enhancing operational intelligence. VIDEO SYNOPSIS® technology is a registered trademark of BriefCam, Ltd. For more information about BriefCam's video content analytics solutions, visit www.briefcam.com.

ATTACHMENT 2: PROPOSAL SUMMARY

QUESTION	ANSWER
What is the company name?	Digi Security Systems
Are you a video analytic developer or a 3 rd party integrator?	3rd Party Integrator
Who is the contact for this proposal?	Sean Hardani
Will this project require the use of a third-party installation and/or integration partner? If so, do they meet the requirements set forth within this document?	No, Digi will provide a full turn-key experience
What is the contact's phone number?	918-824-0001
What is the contact email address?	seanh@digiss.com
If awarded, what is the projected start date?	Planning Phase will start on 9/1/2025
If awarded, what is the projected completion date?	9/30/2025
How many of the Required Functionality capabilities is your solution capable of addressing?	22 Functions
How many of the Preferred Functionality capabilities is your solution capable of addressing?	10 Functions
How many Milestone Certified Integration Technician (MCIT) do you have on staff? (must be one or more)	2 Certified Technicians
How many Milestone Certified Integration Engineers (MCIE) do you have on staff? (must be one or more)	2 Certified Technicians
What is the total project cost?	\$277,992.50
What is the expected recurring annual?	\$19200 for BriefCam Licensing for 100 cameras



REQUEST FOR PROPOSALS

Video Analytics

Executive Summary

IronYun Inc., USA (Vaidio) (prime vendor), with App-Techs Inc. (subcontractor), is pleased to submit a proposal for RFP Video Analytics for Port Freeport for the implementation of a robust, single-site video analytics solution to enhance its existing video surveillance infrastructure. We present the Vaidio solution, which can seamlessly integrate with the current video management system, Milestone XProtect Expert, deployed at the Port Freeport Emergency Operations Center, located at 801 Navigation Blvd, Freeport, Texas 77541. We believe that Vaidio's forward-thinking approach and extensive experience in the competitive AI vision industry, particularly with strengthening operational and security requirements for our customers, make us an ideal technology solutions vendor for Port Freeport. Our commitment to delivering reliable, scalable, feature-rich, accurate, efficient, and cost-effective solutions aligns perfectly with the needs of your organization.

The Vaidio AI Vision Platform delivers next-generation artificial intelligence to monitor and analyze real-time and recorded video. Vaidio can search, monitor, alert, and analyze video with over 30 AI-enabled analytic functions on a single platform. Vaidio detects and alerts on objects, faces, weapons, behaviors, and conditions with market-leading speed and accuracy. Vaidio AI-enabled video analytics and video data analytics add a layer of superhuman intelligence to existing cameras and video infrastructure to improve security, safety, and operational efficiencies across multiple applications and industries. Vaidio is powered by proprietary AI evolved over multiple generations to offer greater accuracy and lower-latency in real-time, and faster forensic video search. The Vaidio Platform supports 30 video analytics that can be used together, including facial recognition, object tracking, weapons detection and more - all using any ONVIF IP camera and integrated fully with Milestone XProtect via SDK/API.

Vaidio can meet all of the analytics features requested by Port Freeport, as well as add additional value by providing a comprehensive video analytics platform. Vaidio's Pro Advanced Software License allows customers to use and flexibly deploy any analytics function supported by the current Vaidio release and is licensed to the total number of cameras to be enabled with Vaidio AI Vision capabilities. The year 1 price of \$154,000, includes Vaidio Core Platform Software, analytics software, software maintenance, hardware appliances (servers) pre-loaded with the software, and hardware maintenance.

Please find enclosed in the documents our response, which includes the following documents:

1. Executive Summary
2. Attachment 2: Proposal Summary



- 3.Detailed Cost Summary
- 4.Compliance - Required & Preferred Functionality
5. Vaidio Proposal
- 6.Project Timeline
7. About Vaidio (vendor) & App-Techs (subcontractor)
- 8.Number of Milestone Certified Tech Members
9. Projected Bandwidth
- 10.Vaidio Rack Space
- 11.System Accuracy
- 12.Proof of Insurance
- 13.Vaidio SLA
- 14.InfoSec Cybersecurity Addendum

Please feel free to reach out to our team to clarify any information or to ask additional questions. We thank you for your time and consideration in reviewing our proposal, and we look forward to having the opportunity to work together as technology partners in providing you with the highest quality solutions.

Sincerely,

A handwritten signature in black ink, appearing to read "Zack Pringle". The signature is fluid and cursive, with a large, stylized "Z" and "P".

Zack Pringle

RSM - Central U.S.

Email: zack.pringle@vaidio.ai

ATTACHMENT 2: PROPOSAL SUMMARY

QUESTION	ANSWER
What is the company name?	Vaidio (fdba IronYun Inc., USA)
Are you a video analytic developer or a 3 rd party integrator?	Video analytic developer
Who is the contact for this proposal?	Zack Pringle
Will this project require the use of a third-party installation and/or integration partner? If so, do they meet the requirements set forth within this document?	Yes, App-Techs is fully certified in Milestone and Vaidio systems.
What is the contact's phone number?	1-708-289-2684
What is the contact email address?	zack.pringle@vaidio.ai info@vaidio.ai
If awarded, what is the projected start date?	July 24, 2025
If awarded, what is the projected completion date?	September 30, 2025
How many of the Required Functionality capabilities is your solution capable of addressing?	All
How many of the Preferred Functionality capabilities is your solution capable of addressing?	12/14 available out-of-the-box (1 requires more information for scoping, 1 requires integration)
How many Milestone Certified Integration Technician (MCIT) do you have on staff? (must be one or more)	4
How many Milestone Certified Integration Engineers (MCIE) do you have on staff? (must be one or more)	1
What is the total project cost?	\$154,000 (year 1)
What is the expected recurring annual?	\$29,900

RFP

Video Analytics for Port Freeport

IDN	Item	Solution Type	Quantity	Unit price (USD)		Term (month)	Billing Frequency	Subtotal for 1 Year	Subtotal for 3 years
1	Vaidio Core Pro Advanced Software License:								
1.1	AI Analytics engines: (admin can allocate licenses / enable analytics as needed) --- Object Detection --- Container ID --- Crowd Detection --- Face Search & Recognition (w/ Age and Gender) --- Intrusion Detection --- License Plate Recognition --- Object Tracking (Counting, Wrong Direction, Dwell Time) --- Person Cross Camera Tracking --- Person Fall --- Personal Protective Equipment --- Smoke & Fire --- Specialized Object (Weapon Detection) --- Vehicle Cross Camera Tracking --- Vehicle Make & Model Recognition	Software	100 --> 200	\$180	per year	36	Annual	\$18,000 --> \$36,000	\$54,000 --> \$108,000
1.2	Core Platform Software: --- Managed via standard web browsers: Chrome, Edge --- Support cameras with standard RTSP (real-time streaming protocol), uploaded videos from computer, and retrieved videos from VMS --- Main functions: object-based search; real-time alert; heatmap --- Other functions: result export, smart hashtag, video playback, live view, privacy protection, outdoor/indoor map, false detection report --- Camera management: camera health management (alert when camera view is blocked/moved/blurry/disconnected), AI model, analytics, object types to detect, ROI (regions of interest), NVR connection, location (GPS map) --- File management: upload video, retrieve video (from NVR) --- User management, support multiple user accounts and user groups with admin-defined permission levels: Camera Control, Video Source Control, AI Engine Control, and Configuration Control; integration with LDAP and Entra ID (SSO) --- System: Web service port configuration, Time, Storage, Mail, LDAP, Log, Audit Trail, License, Setting, AI Model, Utility --- Supports multiple APPs on Android and iOS: Vaidio App allows users to conduct video search and receive notifications from Vaidio Core Platform in real-time; Push Alert notifications into external systems via HTTP; Receive alert signals from 3rd-party devices (IoT devices, sensors, alert systems, etc.) via Vaidio API	Software		included with 1.1		36	Annual		included with 1.1
1.3	Vaidio Data --- Support multiple Vaidio servers with the following business intelligence capabilities to enable decision-making: --- Comprehensive statistics of cameras, people, vehicles, objects, and alert events using Vaidio metadata. --- Use in conjunction with Vaidio analytics engines (Alert Data, LPR/MMR, FRS, and Object Counting)	Software	1 --> 1	included with 1.1		36	Annual		included with 1.1
1.4	Vaidio Command Center --- Central management platform, connect to Vaidio Core --- Includes central Object/Face search, real-time alert, FR/LPR list import to nodes, central license mgmt, node configuration backup/restore, node/camera/list/storage mgmt	Software	1 --> 1	included with 1.1		36	Annual		included with 1.1
1.5	3-Year Term Warranty: --- Annual Software Maintenance Service --- Software hot-fixes and upgrade protection --- 5 x 8 remote technical support	Service	1 --> 1	included with 1.1		36	Annual		included with 1.1
2	Hardware to support Vaidio Core for 200 camera channels (assuming 1080p resolution, 50% traffic and 2-3 AI engines per channel); each server can support at most 245 camera channels. More AI engines per channel will decrease the number of channels.								
2.1	Core Platform server (2U rackmount) with the following specs: - CPU: Dual Intel Xeon-Gold 6430, 2.1GHz (32C/64T) - RAM: 256GB (32GBx8) - GPU: 4x Nvidia L4 - SYS Storage: 3.84TB SSD (3.84TB SATA SSDx2, RAID1) 2SFF U.3 Kit - AI Storage: 12TB (4TB SATA HDD x4, RAID5) - Network Configuration: 1GbE BASE-T x4 or 10GbE BASE-T x2	Hardware	4 --> 4	\$29,750	per server	Perpetual	One-time	\$119,000 --> \$119,000	\$119,000 --> \$119,000

RFP

Video Analytics for Port Freeport

IDN	Item	Solution Type	Quantity	Unit price (USD)		Term (month)	Billing Frequency	Subtotal for 1 Year	Subtotal for 3 years
2.2	Annual Hardware Warranty & Maintenance Service - Appliance/Hardware warranty & maintenance - 5 x 8 remote technical support	Service	4 → 4	\$2,975	per server	36	Annual	\$11,900 → \$11,900	\$35,700 → \$35,700
3	Integration with Milestone VMS - App-Techs Bridge to Milestone Xprotect (BTX) software license	Service	1 → 1	\$1,500	per system		One-time	\$1,500 → \$1,500	\$1,500 → \$1,500
4	Solution installation, setup and configuration	Service	2 → 4	\$1,200	per day		One-time	\$2,400 → \$4,800	\$2,400 → \$4,800
5	User Training	Service	1 → 1	\$1,200	per day		One-time	\$1,200 → \$1,200	\$1,200 → \$1,200

Software license + maintenance and support per camera per month for 3-year term

\$25 → \$20

One time: Hardware fee

\$119,000 → \$119,000

One time: Non-recurring engineering fee + professional services fee

\$5,100 → \$7,500

Total for Year 1:

\$154,000

Total recurring annual:

\$29,900

Total for 3 Years:

\$213,800 → \$270,200

Note:


Pricing is negotiable and presented as a range. Actual values within listed range are to be determined by Port Freeport's needs and further discussions & negotiations between Vaidio and Port Freeport.

List of required features:

ID	Description	Required Function / Capability	Search	Alert	Intel	Vaidio Compliance	Vaidio Component	Comments
The following video analytic functions and capabilities are required:								
R1	Data Source	Action based on specific cameras in Milestone or a video file(s).	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Core Platform Software	
R2	Time Range	Action based on specific time ranges down to the second.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Core Platform Software	
R3	Visual Overlays	Create optional visual data overlay for, but not limited to dwell time, common paths of travel, and heat maps along with boxes identifying objects missing, objects left, people, and vehicles.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Core Platform Software	
R4	Vehicle Classifications	Differentiate between a car, pickup, van, commercial truck, bus, train, motorcycle, bicycle, and boat.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Object Detection	Vaidio vehicle out-of-the-box vehicle classifications include: Bicycle, Bus, Car, Forklift, Jeepney, Motorcycle, Tricycle, Truck, and Tuktuk
R5	License Plate Recognition	Identify license plates in live video and recognize license plates based on watchlists.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	License Plate Recognition	
R6	Vehicle Make and Model	Identify vehicles by make and model.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Vehicle Make & Model Recognition	
R7	People Classifications	Differentiate between male/female and adult/child.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Age & Gender Detection	
R8	Personal Attributes	Identify personal characteristics, such as, but not limited to clothing color, hats, complexion, and/or backpacks.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Object Detection	Vaidio can identify the following attributes: Color and wearable objects including backpack, bag, and luggage
R9	Personal Protection Equipment (PPE)	Identify a person wearing or not wearing PPE, such as, but not limited to safety vest, facial mask, or hard hat.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	PPE Detection	Vaidio PPE detection includes safety vest and hard hat
R10	Color	Identify vehicles, clothing, and objects by color.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Object Detection	
R11	Facial Recognition	Identify images extracted from existing video or photo uploads along with live video face matching for persons on watchlists.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Face Recognition	
R12	Occupancy	Determine the number of people or vehicles in a certain area.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Object Tracking	
R13	Direction	Differentiate the direction of travel for a person or vehicle.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Object Tracking	
R14	Path	Identify the travel path of people and vehicles.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Person & Vehicle Cross Camera Tracking	
R15	Area	Identify objects included or excluded within one or more userdefined polygon areas.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Core Platform Software	
R16	Dwell Time / Loitering	Calculate an object's dwell time for pre-set time periods within a scene.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Object Tracking	



List of required features:

ID	Description	Required Function / Capability	Search	Alert	Intel	Vaidio Compliance	Vaidio Component	Comments
R17	Crossing Line Counting	Count vehicles and people that pass demarcation crossings in a predefined direction(s).	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Object Tracking	
R18	Export	Export searches in standard video formats along with intelligence reports in PDF to support partner collaboration.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Core Platform Software	
R19	Real Time Processing	Analysis of video data as it is being captured.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes, available today	Core Platform Software	
R20	On Demand Processing	Review and analyze previously recorded video content based on specific criteria, events, or queries.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Core Platform Software	
R21	Motion Detection	Detect physical movement for a given area.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Intrusion Detection	
R22	Custom Classifications w/ No Scripts	Create custom classes by uploading a few visual examples with no scripts.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, short-term custom dev		Vaidio provides a Vaidio DIY tool for customer to create custom labels / classes for object types that are not included out-of-the-box in the Vaidio Core Platform Software
The following video analytic functions and capabilities are preferred, but not required:								
P1	Aerial Classification	Differentiate between a helicopter, airplane, and drone.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, short-term custom dev	Object Detection	
P2	 Video Synopsis	Simultaneously view objects that have appeared at various times during a search or alert.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Yes, available today	Core Platform Software	Vaidio allows users to search for specific objects or events, or alert on specific objects - only relevant matches will appear in the search or event results for simultaneous viewing
P3	Bookmark	Bookmark objects of interest.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Yes, available today	Core Platform Software	
P4	Pandemic Proximity Detection	Detect the distance between individuals over time and location for measuring compliance with physical distancing mandates and contact tracing.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Need more information		
P5	Crowd Counting	Count the number of people in sizeable crowds over 50 in a predefined area.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Crowd Detection	
P6	Speed	Calculate an object's actual speed.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Object Tracking	
P7	Fall Alert	Detect when an individual falls.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Person Fall	
P8	Run Alert	Detect when an individual runs.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Object Tracking	
P9	Gun Detection	Detect long guns and pistols in realtime.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Specialized Object (Weapons)	
P10	Aggression Detection	Detect verbal aggression in realtime.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	Not in scope	Vaidio does not analyze sound / verbal language, but can integrate with audio sensors
P11	Smoke & Fire Detection	Detect smoke and/or fire.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Intrusion Detection (for Fire & Smoke)	
P12	Wait Times	Determine the average wait time for vehicles and people at check-in point and alert when expected wait time is exceeded.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Object Tracking	

- P5 "Beer Lines"
 - P6
 - P7
 P8
 - P9
 P10 "Crowd Fighting?"
 - P11

List of required features:

ID	Description	Required Function / Capability	Search	Alert	Intel	Vaidio Compliance	Vaidio Component	Comments
P13	Tamper Detection / Image Change	Detect a major change in the camera view such as an obstruction, power cut, or spray painted etc.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, available today	Core Platform Software	
		Locate shipping containers by scanning for a specific identification number on the container.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
P14	Container Identification					Yes, available today	Container ID	



REQUEST FOR PROPOSALS Video Analytics

Video Analytic Solution

General Requirements

Driven by artificial intelligence and deep learning, the video analytics shall be capable of deriving searchable, actionable, and quantifiable intelligence from live or recorded video content. **Yes**

The Vendor shall provide all required analytical functions described within this document in a single solution. **Yes**

The proposed video analytics solution shall incorporate a convolutional neural network (CNN) architecture to enable advanced image processing and pattern recognition capabilities. The CNN shall be optimized to ensure high accuracy, efficiency, and scalability in analyzing video data, aligning with the operational requirements of the surveillance system. **Yes**

The interface shall utilize a centralized administration, which will allow users to view and activate cameras, configure hosts, GPUs, and services from a single web interface. **Yes**

The video analytic solution shall have the ability to schedule continuous, one-time, daily, or weekly automatic video processing for each VMS video source. **Yes, needs further discussion with Port Freeport stakeholders to determine the scheduling needs. Users can import video files from Milestone VMS and apply AI analytics to the video file as if it were a real-time camera.**

An on-premises solution is preferred, but if a cloud-based solution is proposed, the servers shall be dependable, secure, and located in the United States, Switzerland, or Canada. The server solution shall have built-in redundancy in the event connectivity is lost with the main server. The hardware and traffic shall have continuous security monitoring to quickly identify malicious or unauthorized behavior. **N/A. Vaidio will be deployed on-premises.**

On-premises solutions must contain redundant power supplies and related hardware to assure proper bandwidth needs. **Yes**

The video analytic solutions shall be integrated with 100 cameras in the Milestone environment. The servers and hardware shall be expandable to 200 cameras for future growth. **Yes**



Overall system accuracy shall be greater than 95%. **Yes, please see Vaidio System Accuracy document.**

At minimum, the solution shall allow five (5) concurrent users. **Yes**

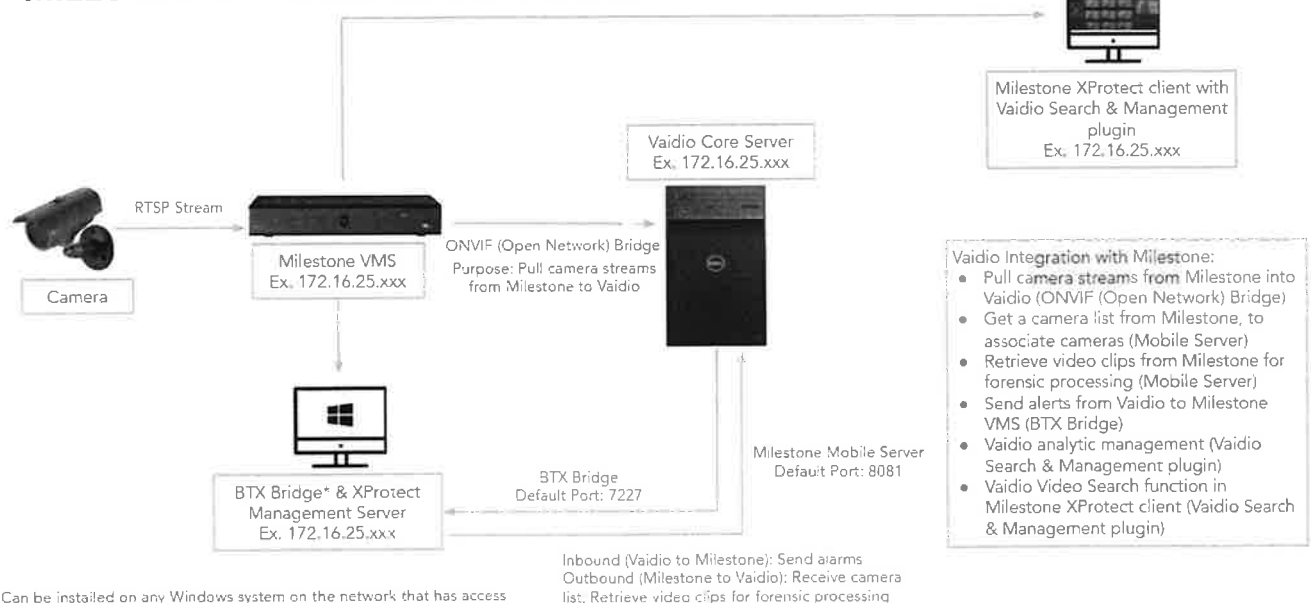
The proposed video analytics solution shall leverage an open platform architecture to ensure seamless integration with a diverse array of Video Management Systems (VMS) and camera models. **Yes, Vaidio is an open platform with a RESTful API for seamless integration with third-party systems.**

Compatibility

The user interface client/software shall be Windows 10 and Windows 11 compatible. **Yes, accessing the Vaidio user interface does not require a separate client / software download. Vaidio UI is compatible with Windows 10 and Windows 11 and on standard web browsers: Google Chrome, Microsoft Edge.**

The video analytic solution shall be compatible with Milestone XProtect Smart Client 2023 R3 and newer. **Yes, please see diagram below:**

MILESTONE NETWORK ARCHITECTURE





The video analytic solution shall be compatible with Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari on Mac and iPad. **Yes; however, for best performance, we recommend Google Chrome and Microsoft Edge web browsers.**

The video analytic solution shall be compatible with H.263, H.264, H.265, H.265/HEVC, and MPEG-4 codecs. **Vaidio is compatible with H.264, H.265, MJPEG, MPEG1, MPEG2, MPEG4, VC1, VP8, and VP9 codecs.**

The video analytic solution shall be compatible with AXIS cameras. **Yes, Vaidio is compatible with any ONVIF-compliant IP camera, including AXIS cameras.**

The video analytic solution shall be compatible with .264, .ASF, .AVI, .MOV, .MP3, .MP4, .WMV, and .RAW video file formats. **Vaidio is compatible with MP4, MPEG, M4V, MPG, MOV, WMV, ASX, AV1, OGM, OGV, and WebM video file formats.**

Compliance

The video analytic solution shall be designed, developed, and coded in the United States or an allied nation, but it is preferred that the provider has its headquarters in the United States. If produced outside the United States, the solution shall have customer and technical support in the United States. **Yes. Vaidio headquarters is located at 263 Tresser Blvd., Floor 9, Stamford, CT 06901. Customer and technical support personnel are located throughout the United States, including Houston, TX. The technical support office is located at 245 Amity Rd., Suite 208, Woodbridge, CT 06525.**

If using off site servers and/or storage, the server location, hardware, and environment shall be NIST compliant. **N/A**

The proposed video analytics shall include the following capabilities:

- Search: Video search capability through the utilization of cross-camera video search and filtering, based on, but not limited to object classes and attributes, metadata, activity, dwell time, common paths, and heatmaps. **Yes**
- Alert: Real time alerts via email, text, and/or app based on object classification and recognition filter combinations to increase situational awareness and deliver critical, time-sensitive intelligence. **Yes, real-time alerts via email, app, and/or Milestone.**
- Intelligence: Operational and business intelligence, which visualizes object movement, demographic segmentations, behavior trending, hotspots, and object interactions with customizable, easy-to-use dashboards for data analysis, as well as tools for auto-generating and prioritizing relevant data points and charts. **Yes**



All proposed facial recognition technology solutions shall fully comply with the standardized datasets of images established by the National Institute of Standards and Technology (NIST).
Yes

Required Functionality

See Vaidio Compliance - Required & Preferred Functionality document.

Preferred Functionality

See Vaidio Compliance - Required & Preferred Functionality document.

Miscellaneous Items

Training

All proposals shall include at least eight (8) hours of training on the function and utilization of the video analytic solution. The training program exclusively addresses the operation of the analytical solution and does not encompass decision management, including response procedures and protocols. **Yes**

The training can be in person or by video conference. **Yes**

Regulatory Codes

The Vendor shall be responsible for meeting all applicable local, state, and federal codes. **Yes**

The Vendor and its agents, employees, contractors, and invitees shall comply with any and all Port safety and security policies in effect or as levied from time to time by Port Freeport. Should any of these parties cause the Port to be levied a fine due to act or omission, physically or verbally, of agents, employees, contractors or invitees, the Vendor shall be responsible for such fine plus an administration fee. **Yes**

When required, the Vendor shall be responsible for providing all applicable personal protective equipment (PPE). **Yes**

The Vendor shall follow all applicable OSHA and NFPA standards as required by local, state, and federal rules and regulations. **Yes**



Workmanship & Quality

Cable Management

All network cabling shall be inspected and tested under the ANSI/TIA 568 C.2 standard with a certified tester. For all non-networking cable, the cable shall be visually inspected for any damage. Additionally, the cabling shall be tested for shorts and ground faults. **Yes**

The Vendor must provide evidence that the tester(s) used has a current calibration less than a year old. **Yes**

All cables shall be one continuous run from device to device (i.e., no slicing). Extenders are allowed if needed. **Yes**

All enclosures, equipment, cabling, and connections installed in non-environmentally controlled areas (e.g., outdoor locations) shall be fully weather sealed to ensure protection against environmental elements and maintain operational integrity. **Yes**

Warranty

The Vendor shall warrant all hardware, software, cabling, and ancillary equipment against defects in materials, workmanship, and performance for a minimum period of one (1) year from the date of final commissioning and acceptance by the contracting authority. **Yes, included in the annual warranty & maintenance service.**

The warranty shall encompass:

- Full repair or replacement of defective hardware components, including servers, network switches, cabling, and other ancillary equipment, at no additional cost to the contracting authority. **Yes, included with the annual warranty & maintenance service.**
- Correction of software defects, including bugs, performance issues, or integration failures, through patches, updates, or reconfigurations, ensuring compatibility with the existing video management system. **Yes, included with the annual warranty & maintenance service.**
- Labor and travel expenses are associated with warranty-related repairs or replacements. **Yes, included with the annual warranty & maintenance service.**

The Vendor shall provide a guaranteed response time of no more than four (4) to eight (8) hours for critical issues affecting system functionality, with on-site support initiated within twenty-four (24) hours of issue notification. Non-critical issues shall be addressed within two (2) business



days of notification, with resolution completed within five (5) business days. With Port Freeport's approval, additional time may be requested in the event a supply chain issues causes a delay more than five (5) business days. **Yes. Remote support initiated within 24 hours of issue notification for critical issues affecting system functionality. Please see Vaidio's standard Service Level Agreement and Service Definition Document.**

A dedicated point of contact and technical support hotline shall be provided for warranty-related inquiries and issue reporting. **Yes. When any issue arises that requires information or support from Vaidio, the end-user customer is responsible for submitting a formal written request for service in the form of a ticket in the Support Portal (vaidio.ai/support). Please see Vaidio's standard Service Level Agreement and Service Definition Document.**

The Vendor shall warrant that the installed solution meets or exceeds the functional and performance requirements specified in the Request for Proposal (RFP) for the duration of the warranty period. In the event of non-compliance, the Vendor shall implement corrective measures, including hardware or software modifications, at no cost to the contracting authority. **Yes**

The Vendor shall provide detailed warranty documentation, including terms, conditions, and procedures for submitting claims, as part of the project deliverables. **Yes.**

Vaidio Warranty / Maintenance Service provides comprehensive coverage for appliance hardware warranty, software license agreements, software hot-fixes, version upgrade, and technical support under a single, common set of agreements, and processes.

Vaidio Warranty Service includes:

- 1. Hardware Warranty Service (applicable for appliance product)**
 - DOA/RMA process for hardware parts repair and/or replacement
 - Turnaround time within 14 working days upon DOA/RMA request
- 2. Software Maintenance Service**
 - Software License Agreement
 - Software hot-fixes
 - Software version upgrade protection
- 3. Technical support**
 - 5x8 remote technical support
 - Service channels: Support Portal

Warranty / Maintenance Service Extension



- **Warranty / Maintenance Service option is generally renewable to extend the service period on an annual basis.**
- **The Warranty / Maintenance Service is available to extend if it is under effective service period.**
- **If the Warranty / Maintenance Service is not extended by the due date the service is considered lapsed, support will be systematically terminated.**
- **To reinstate the service after lapsed, the customer must pay the full Warranty / Maintenance Service period expense to Vaidio, which includes all Warranty / Maintenance Service expiration period expense.**

Hardware Warranty Terms

1. **IronYun's hardware products, including all appliances and storage modules/boxes, are under warranty against defects in materials and workmanship during the warranty service period.**
2. **Exceptions to #1 include cases where the defect is the result of misuse or damage by the user.**
3. **For individual Vaidio appliance warranty coverage, please refer to the warranty date on the license page of the Vaidio software.**
4. **If the product is repaired or replaced, the repaired or replaced product will continue to be under warranty for the remaining time of the original warranty period, or three months from the date of repair or replacement, whichever is longer.**
5. **When the product is sent to IronYun, the period of maintenance before and after the repair or replacement is calculated as a part of the warranty period.**

Dead on Arrival (DOA)

The defective hardware product that fails to work normally upon arrival at the customer's side is considered DOA.

1. **The term applies to 30 days from the date of shipment from IronYun.**
2. **IronYun will pay all delivery fees for the DOA product shipment.**

Return Merchandise Authorization (RMA)

1. **Customer will pay the delivery fee for the RMA product to be shipped to IronYun.**
2. **IronYun will pay the delivery fee for the RMA product to be returned to Customer.**
3. **Warranty of repaired and replaced products**



- **Products that have been repaired or replaced are warranted only for the unexpired portion of the original warranty period, or for three months from the date of the repair/replacement, whichever is longer.**

DOA/RMA Process

- 1. Customer files a Support Portal ticket and fills in the product serial number.**
- 2. IronYun Support Center checks the warranty status based on the product serial number.**
- 3. If under warranty, IronYun Support Center will reply to the ticket with the DOA/RMA number via Support Portal or email.**
- 4. Customer ships the unit to IronYun with the DOA/RMA number.**
- 5. IronYun will repair and ship the unit back to Customer within 14 working days.**

Replacement parts shall be new, meet original equipment manufacturer (OEM) specifications, and be compatible with the installed system.

The Vendor shall warrant that any training provided as part of the project remains applicable to the system throughout the warranty period, with additional training sessions offered at no cost if the software updates significantly alter system operation. **Yes**

Maintenance

A comprehensive maintenance agreement for software and network hardware, such as those supporting an advanced camera analytics solution, shall include the following provisions to ensure system reliability, performance, and compliance with operational requirements through October 31, 2026. **Yes**

The agreement shall clearly define the covered components, including all software applications, firmware, servers, network switches, cabling, and ancillary hardware installed as part of the system. Maintenance services shall encompass preventive maintenance, corrective maintenance, software updates, and technical support. **Yes, see above Warranty & Maintenance terms.**

The Vendor shall conduct regular preventive maintenance, including system health checks, performance optimization, and hardware inspections, at least quarterly or as recommended by equipment manufacturers. Preventive maintenance schedules shall be coordinated with the contracting authority to minimize operational disruptions. **Yes, please see Vaidio SLA document.**



The Vendor shall provide all software updates, patches, and firmware upgrades to maintain system security, performance, and compatibility with the existing video management system (e.g., Milestone XProtect Expert). Updates shall be tested in a controlled environment prior to deployment to prevent unintended disruptions. The agreement shall ensure that all software licenses remain valid and supported throughout the maintenance period. **Yes**

The Vendor shall perform repairs or replacements for defective hardware components, including servers, network switches, and cabling, at no additional cost during the maintenance period. Replacement parts shall be new, meet original equipment manufacturer (OEM) specifications, and be compatible with the installed system. The Vendor shall maintain an inventory of critical spare parts to ensure timely repairs. **Yes, see above Warranty & Maintenance terms.**

The Vendor shall provide a dedicated point of contact for maintenance-related inquiries and issue escalation. Support shall include remote diagnostics, troubleshooting, and, when necessary, on-site technician dispatch. The agreement shall specify whether support is available 24/7 or limited to business hours, with clear escalation procedures for after-hours emergencies. **Yes, please see standard Vaidio SLA document.**

The Vendor shall ensure that all maintenance activities comply with applicable industry standards, data protection regulations, and the contracting authority's security policies. Software updates shall address known vulnerabilities, and the Vendor shall provide documentation of compliance with cybersecurity best practices. **Yes, please see the Cybersecurity and Information Security Policies and Operations of IronYun (Vaidio) document.**

The agreement shall specify the initial term (e.g., one year) and options for renewal, including any price escalation clauses. Termination conditions, including notice periods and obligations for transitioning to a new Vendor, shall be clearly defined. **Yes, please refer to the Vaidio EULA (<https://www.vaidio.ai/eula>) and Terms and Conditions (<https://www.vaidio.ai/terms-and-conditions>).**

The agreement shall detail all costs, including fixed fees for preventive maintenance, rates for corrective maintenance, and any additional charges for after-hours support or expedited repairs. Costs for software updates and licenses shall be included in the agreement to avoid unforeseen expenses. **Yes, see above Warranty & Maintenance terms.**

The Vendor shall maintain adequate insurance coverage, including general liability and professional liability, to cover potential damages arising from maintenance activities. The agreement shall specify the Vendor's liability for system downtime or data loss caused by maintenance errors. **Yes, please see the Certificate of Liability Insurance document.**



The Vendor shall disclose any subcontracting arrangements and ensure that all personnel performing maintenance are qualified and trained in the relevant technologies. **Yes, Vaidio's subcontractor for this project is App-Techs. The personnel are fully certified in both Milestone and Vaidio systems.**



Project Timeline

Project Timeline Overview

Phase	Start Date	End Date	Duration	Key Activities
Planning Phase	July 24, 2025	August 7, 2025	~2 weeks	RFP award, Rapid requirements finalization, kickoff
Installation Phase	August 8, 2025	September 15, 2025	~5.5 weeks	Hardware shipping & installation, network & software setup, analytics configuration
Commissioning Phase	September 16, 2025	September 30, 2025	~2 weeks	Testing, calibration, staff training
Project Completion	September 30, 2025	-	-	Final acceptance & handover

Planning Phase (July 24 - August 7, 2025)

Objective:

- Contract awarded on July 24
- Rapidly finalize technical requirements, scope of work, & conduct site surveys if required
- Conduct project kickoff and initial site coordination

Milestone:

- Scope of work & requirements gathering complete by August 7, 2025

Installation Phase (August 8 - September 15, 2025)

Objective:

- Order servers & install Vaidio software onto servers



- Ship servers to Port Freeport Emergency Operations Center, located at 801 Navigation Blvd, Freeport, Texas 77541
- Port Freeport to provide list of cameras to be added to Vaidio, including IP address, RTSP stream URL (if applicable), credentials, and desired analytics per camera stream
- After server arrival and rackmount, add cameras to Vaidio
- Perform initial Vaidio analytics configuration
- Connect Vaidio to Milestone VMS

Milestone:

- Server installation complete, analytics setup, & system ready for commissioning by September 15, 2025

Commissioning Phase (September 16 - September 30, 2025)

Objective:

- Comprehensive system testing in conjunction with Port Freeport (analytic alerts, Milestone integration, etc.)
- Calibration of system in conjunction with Port Freeport (fine-tuning detection zones, adjusting alerts)
- System training with Port Freeport security operators, IT teams, and other stakeholders

Milestone:

- System fully commissioned & operational by September 30, 2025

Project Completion & Handover (September 30, 2025)

Objective:

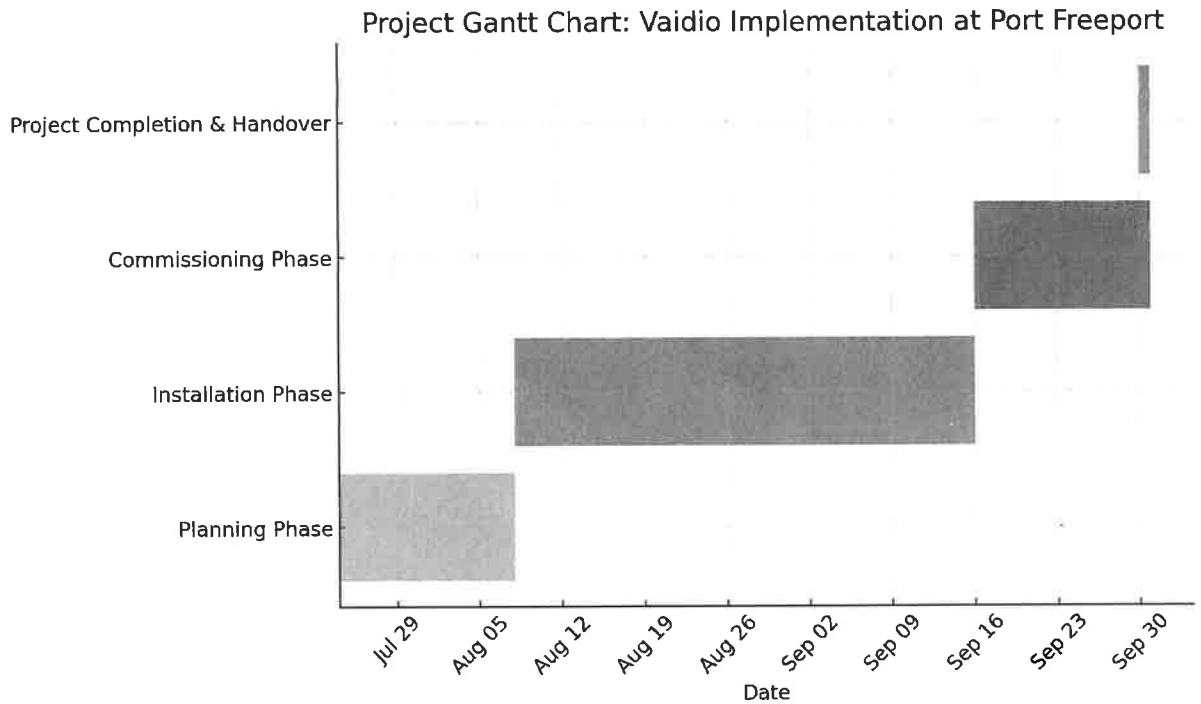
- Final system review with Port Freeport
- Handover of documentation and support SLA

Milestone:

- Formal project closeout on September 30, 2025



Project Gantt Chart: Video Analytics RFP





REQUEST FOR PROPOSALS

Video Analytics

About Vaidio (Vendor & Prime Contractor)

IronYun Inc., USA (Vaidio) was incorporated in 2015 in Delaware as a C Corporation. Vaidio headquarters are at 263 Tresser Blvd., Floor 9, Stamford, Connecticut 06901. Vaidio's mission is to solve real world problems and to create value for our customers with our advanced AI Vision platform. Including the incubation period prior to incorporation, Vaidio has 30 years of history and experience in the field of AI Vision. With that heritage in mind, our world-class team has evolved the Vaidio AI Vision platform over multiple generations to make it the industry's most accurate, resource-efficient, context aware, comprehensive, and mature AI Vision platform in the industry.

Vaidio was recognized as a Major Player in the 2021 JDC Worldwide Video Analytics MarketScope. In 2019, Vaidio received a grant from the United States Department of Defense Combating Terrorism Technical Support Office (US DoD CTTSO): "10/01/2019 BAA 19- S-3011 - The Personal Protection Subgroup awarded an \$857,362.00 contract to IronYun USA, Inc. to develop a 360-degree anomaly detection system that uses an artificial intelligence algorithm to provide a high level of situational awareness to the user." Vaidio AI Vision Platform won the coveted SIA (Security Industry Association) New Product Showcase Awards at ISC West in 2020, 2021, 2023, 2024, and 2025.

The Vaidio AI Vision Platform delivers next-generation artificial intelligence to monitor and analyze real-time and recorded video. Vaidio can search, monitor, alert, and analyze video with over 30 AI-enabled analytic functions on a single platform. Vaidio detects and alerts on objects, vehicles, behaviors, and conditions with market-leading speed and accuracy. Vaidio AI-enabled video analytics and video data analytics add a layer of superhuman intelligence to existing cameras and video infrastructure to improve security, safety, and operational efficiencies across multiple applications and industries.

About App-Techs (Subcontractor)

App-Techs Corporation (App-Techs) sells, installs, supports, and maintains video security systems, access control networks, and security network infrastructure. We also specialize in security system integrations, which gives clients the ability to combine the inputs and outputs from multiple security systems into a unified user interface. App-Techs is located at 505 Willow Lane, Lancaster, PA 17601.



App-Techs specializes in the development of security-related software and Milestone integrations such as video and audio analytics, access control and security systems, and server and network health monitoring. With both hardware and software expertise, App-Techs creates and develops novel security solutions when none exist in the marketplace.

Technicians at App-Techs are Milestone-certified and maintain numerous technical certifications and government contractor approvals. In 2021, Dan Fritsch received recognition from Milestone Systems as a “Milestone Developer Champion.” App-Techs is an authorized vendor with various state and federal agencies, including GSA (and SAM), PEPPM, COSTARS, and PA eMarketplace (ITQ). App-Techs is fully trained / certified by Vaidio (IronYun).

Our customers include local, state and federal governments, schools, colleges, manufacturing facilities, corporate campuses, civic and entertainment venues, non-profits, retail, and residential.

App-Techs is committed to implementing solutions that align with client objectives and deliver good business value. We continuously leverage our computer, networking, wireless, software, and product knowledge to deliver superior results that meet clients’ needs and budgets.



REQUEST FOR PROPOSALS

Video Analytics

Milestone Certified Tech Members

- Milestone Certified Integration Technician (MCIT) - 4 (App-Techs, subcontractor)
- Milestone Certified Integration Engineer (MCIE) - 1 (App-Techs, subcontractor)
- Milestone Certified Design Engineer (MCDE) - 2 (App-Techs, subcontractor)



REQUEST FOR PROPOSALS

Video Analytics

Vaidio Projected Bandwidth

Projected bandwidth (i.e., Mbps or Gbps) required to implement video analytics on 100 cameras, assuming 1920 x 1080p resolution (2MP) ([utilizing bandwidth calculator](#)):
292.97 Mbps

Projected bandwidth (i.e., Mbps or Gbps) required to implement video analytics on 100 cameras, assuming 2560 x 1600p resolution (4MP) ([utilizing bandwidth calculator](#)):
390.63 Mbps

Projected bandwidth (i.e., Mbps or Gbps) required to implement video analytics on 200 cameras, assuming 1920 x 1080p resolution (2MP) ([utilizing bandwidth calculator](#)):
585.94 Mbps

Projected bandwidth (i.e., Mbps or Gbps) required to implement video analytics on 200 cameras, assuming 2560 x 1600p resolution (4MP) ([utilizing bandwidth calculator](#)):
781.25 Mbps

Bandwidth calculator: <https://www.digiever.com/support/calculator.php>



REQUEST FOR PROPOSALS

Video Analytics

Vaidio Rack Space Needed

Vaidio requires rackspace to support 4x 2U (8 LFF) rackmount servers.

Network configuration per server: 1GbE BASE-T x 4 or 10GbE BASE-T x 2



REQUEST FOR PROPOSALS

Video Analytics

Vaidio System Accuracy

Overall system accuracy shall be greater than 95% for the following analytic engines, provided that the following conditions are met:

Object Detection

- Object size is at a minimum 30 pixels within the camera FoV
- Camera: Minimum 1080p resolution

Age & Gender Detection

- Lighting: Normal, uniform; recommend camera with strong Wide Range feature for bright backgrounds
- Movement: Normal walking speed
- Camera Placement: Position as close to eye level as possible (i.e., 6-8 ft high for clear face profiles)
- Head Pose: $\leq 35^\circ$ for detection, $\leq 15^\circ$ for recognition
- Image Quality: $\geq 1080p$ resolution
- Face Size: ≥ 160 ppf (240 ppf recommended) OR 80 px min (120 px recommended)

Container ID

- Camera: Minimum 1080p resolution
- Character Size: At least 16 pixels wide for clear detection
- Placement: Position camera close to container ID level (avg. height 8-9 ft / 2.5-2.8m)

Crowd Detection

- Person or head size are at a minimum 30 pixels within the camera FoV
- Camera: Minimum 1080p resolution



Face Recognition

- Lighting: Normal, uniform; recommend camera with strong Wide Range feature for bright backgrounds
- Movement: Normal walking speed
- Camera Placement: Position as close to eye level as possible (i.e., 6-8 ft high for clear face profiles)
- Head Pose: $\leq 35^\circ$ for detection, $\leq 15^\circ$ for recognition
- Image Quality: $\geq 1080p$ resolution
- Face Size: ≥ 160 ppf (240 ppf recommended) OR 80 px min (120 px recommended)

Intrusion Detection (includes Smoke & Fire Detection)

- Object size is at a minimum 30 pixels within the camera FoV
- Camera: Minimum 1080p resolution

License Plate Recognition

- Camera: Minimum 1080p resolution
- Character Size: At least 16 pixels wide for clear detection (e.g., a plate with 6 alphanumeric characters should be at least 100 px wide for clear detection)
- Camera placement for best LPR results:
 - Place camera at an angle as close to the license plate level as possible
 - Horizontal angle $< 25^\circ$ (i.e., angle between the line of sight (straight line from license plate to camera) and the ground)
 - Side angle $< 25^\circ$ (i.e., angle between the line of sight and the vehicle's direction of movement)
- Typical best-performance deployment: Cameras at parking lot entrances and traffic lights, cars moving at < 10 mph, and detecting max. 3 lanes of vehicles at the same time

Object Tracking (includes Counting, Occupancy, Dwell, and Wrong Direction)

- Object size is at a minimum 30 pixels within the camera FoV
- Camera: Minimum 1080p resolution

Person Cross Camera Tracking

- Person size is at a minimum 128 pixels within the camera FoV
- Camera: Minimum 1080p resolution



Person Fall

- Object size is at a minimum 100 pixels within the camera FoV
- Camera: Minimum 1080p resolution
- Camera Placement: Ensure full-body view; avoid overhead angles

Personal Protection Equipment (PPE)

- Object size is at a minimum 100 pixels within the camera FoV
- Camera: Minimum 1080p resolution

Specialized Object (Weapons Detection)

- Handgun size is at a minimum 30 pixels per target or 60 pixels per foot within the camera FoV
- Rifle size is at a minimum 30 pixels per target or 9 pixels per foot within the camera FoV
- Camera: Minimum 1080p resolution

Vehicle Cross Camera Tracking

- Vehicle size is at a minimum 128 pixels within the camera FoV
- Camera: Minimum 1080p resolution

Vehicle Make & Model Recognition

- Vehicle size is at a minimum 200 pixels within the camera FoV
- Camera: Minimum 1080p resolution



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

06/07/2021

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an **ADDITIONAL INSURED**, the policy(ies) must have **ADDITIONAL INSURED** provisions or be endorsed. If **SUBROGATION IS WAIVED**, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Hiscox Inc. 520 Madison Avenue 32nd Floor New York, NY 10022	CONTACT NAME: PHONE (A/C, No, Ext): (888) 202-3007 FAX (A/C, No): E-MAIL ADDRESS: contact@hiscox.com																					
INSURED IronYun, Inc. USA 263 Tresser Blvd, Fl 9 Stamford CT 06901	<table><tr><th colspan="2">INSURER(S) AFFORDING COVERAGE</th><th>NAIC #</th></tr><tr><td>INSURER A:</td><td>Hiscox Insurance Company Inc</td><td>10200</td></tr><tr><td>INSURER B:</td><td></td><td></td></tr><tr><td>INSURER C:</td><td></td><td></td></tr><tr><td>INSURER D:</td><td></td><td></td></tr><tr><td>INSURER E:</td><td></td><td></td></tr><tr><td>INSURER F:</td><td></td><td></td></tr></table>	INSURER(S) AFFORDING COVERAGE		NAIC #	INSURER A:	Hiscox Insurance Company Inc	10200	INSURER B:			INSURER C:			INSURER D:			INSURER E:			INSURER F:		
INSURER(S) AFFORDING COVERAGE		NAIC #																				
INSURER A:	Hiscox Insurance Company Inc	10200																				
INSURER B:																						
INSURER C:																						
INSURER D:																						
INSURER E:																						
INSURER F:																						

COVERAGES**CERTIFICATE NUMBER:****REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PROJECT <input type="checkbox"/> LOC OTHER:			UDC-4551181-CGL-21	07/22/2021	07/22/2022	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 100,000 MED EXP (Any one person) \$ 5,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ S/T Gen. Agg. \$
	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY						COMBINED SINGLE LIMIT (Ea accident) \$ BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
	UMBRELLA LIAB <input type="checkbox"/> OCCUR EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED RETENTION \$						EACH OCCURRENCE \$ AGGREGATE \$ \$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) <input type="checkbox"/> Y/N If yes, describe under DESCRIPTION OF OPERATIONS below	N/A					PER STATUTE <input type="checkbox"/> OTH-ER <input type="checkbox"/> E.L. EACH ACCIDENT \$ E.L. DISEASE - EA EMPLOYEE \$ E.L. DISEASE - POLICY LIMIT \$

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER**CANCELLATION**

WESCO Distribution, Inc. & Subsidiaries
225 W Station Square Drive, Suite 700
Pittsburgh, PA 15219
ATTN: Data Governance

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

© 1988-2015 ACORD CORPORATION. All rights reserved.



Service Level Agreement and Service Definition Document

1. Document Information	2
1.1 Scope and Objectives	2
2. Support & Training	2
2.1 Training Materials	2
3. Incidents	2
3.1 Definition	2
3.2 Incident Support Levels	3
3.3 Availability	3
3.4 Organizational Impact and Response Times	4
4. Service Requests	5
4.1 Definition	5
4.2 Software Configuration Management (Vaidio and other key software modules)	5
4.3 Security Management	5
4.4 Service Level Management	6
4.5 Data Maintenance	6
5. Backup and Restore	6
5.1 Definition	6
5.2 Key Component Backup and Restore Service Levels	6
6. Standard Operating Procedures (SOP)	7



1. Document Information

1.1 Scope and Objectives

This Service Level Agreement and Service Definition Document (the "Agreement") contains key metrics and requirements for Vaidio's services and support standards to End-user Customers of Vaidio's licensed software.

This Agreement applies to all products and services provided by Vaidio except where superseded by service-specific SLAs. This Agreement may be modified by Vaidio to accommodate service-specific SLAs in its discretion via the addition of written amendment(s) signed by a duly authorized representative of Vaidio and appended to this Agreement.

The objectives of this document are to describe the base level of service and the means of providing consistent service at a predefined level of quality.

2. Support & Training

2.1 Training Materials

Vaidio provides materials for End-user Customers' technical support teams to support their customers who have purchased Vaidio. Vaidio offers technical information including data sheets, user guides and an FAQ page, as well as online training materials and certification courses, which can be found in Vaidio Partner Portal (<https://www.Vaidio.com/partner-resources/resource-library>).

3. Incidents

3.1 Definition

Incidents are generally an unplanned interruption or a request to add, modify or remove something. Priority levels are assigned to help Vaidio prioritize incidents based on end-user urgency and organizational impact. The urgency is determined by the end-user personnel, and the impact is determined by Vaidio personnel.



3.2 Incident Support Levels

Level	Description	Responsibility
Level 1	Typically encompasses simple issues such as software access, video source connection, standard analytic configuration, and basic troubleshooting on any device that needs to be installed, plugged in, or powered up.	Integrator partner
Level 2	Encompasses in-depth troubleshooting and technical analysis of incidents involving the configuration and provisioning of advanced AI Video Analytics engines. Due to the large number of analytics provided by Vaidio, the deployment of certain analytics may require support from Vaidio solution architects and/or system engineers.	Vaidio
Level 3	Incidents such as software bugs or work-around solutions involving special software patches or fixes to existing customer installations.	Vaidio

3.3 Availability

Description	Essential Service Level
Support scope	10h x 5d
Support days	Monday - Friday
Support hours	8 a.m. - 6 p.m. US Eastern Time: Eastern Standard Time (UTC-05:00) Eastern Daylight Time (UTC-04:00)
Environment availability*	99%
Maintenance windows	Monthly, the second Sunday of the month: 1:00 a.m. - 4:00 a.m. U.S. Eastern Time
Application availability	N/A

* Number of hours availability divided by number of hours in the primary support scope, excluding planned maintenance window time



3.4 Organizational Impact and Response Times

Impact	Level 1 and Level 2 Technical Support	Level 3 Technical Support
Critical System-wide impact; high visibility; no alternative option.	15-min response 4-hr resolution E.g.: network failure, data center outage	15-min response 8-hr resolution E.g.: OS crash
Major impact System-wide impact; high visibility; an alternative option can be deployed	15-min response 8-hr resolution (after deploying the alternative) E.g.: power outage with backup generator	15-min response 8-hr resolution (after deploying the alternative) E.g.: critical bug in software
Moderate impact Individual account / location affected; limited visibility	1-hr response 5-day resolution E.g.: local server failure; single user unable to access application; accidental deletion of user account	2-hr response 5-day resolution E.g.: location with unique setup that affects software performance
Minor impact Users have functionality and normal performance when workaround is followed	1-day response End-user Customer to notify Vaidio to discuss resolution	1-day response Resolution to be discussed with End-user Customer and scheduled E.g.: software improvement suggestion
Emergency requests Unique business situation	Commercially reasonable effort	Commercially reasonable effort



4. Service Requests

4.1 Definition

Service Requests are requests that follow a predefined workflow and are service specific. They are designed to gather all necessary information through a form that is assigned directly to a responsible team.

Service Requests may cover product specification, procurement, licensing, hardware server and storage requirements.

4.2 Software Configuration Management (Vaidio and other key software modules)

Description	Essential Service Level
Vaidio system software corrective maintenance (Vaidio Core)	As required to resolve critical- or major-impact problems
Operating system and K8s system software preventative maintenance (patches aged 60 days and deemed critical by customers)	Quarterly update
Vaidio Website, Web portal	N/A

4.3 Security Management

Description	Essential Service Level
Vaidio Core and Vaidio K8s security and system management parameter review	Quarterly
Add, change, or disable key servers, routers, appliance user ID, changes retained for one year	Quarterly
Emergency user ID or application resource control requests based on potential threat	Within 1 hour of receipt
Reset/change user password from authorized	Within 30 minutes of receipt during coverage



requestor	hours
-----------	-------

4.4 Service Level Management

Description	Essential Service Level
Service level reports	On-demand
Service level review	On-demand

4.5 Data Maintenance

Description	Essential Service Level
Data requested (by end-user) to be exported, e.g., due to legal or law enforcement request	Within 24 hours during coverage hours
Data requested (by end-user) to be deleted, e.g., due to legal or law enforcements request	Within 24 hours during coverage hours

5. Backup and Restore

5.1 Definition

Backup is the process of copying computer data, such as a volume, database, or virtual machine from a registered server to a backup container or vault. Restore is the process of restoring computer data from a backup container or vault to a registered server.

Service Levels for Backup and Restore are more common in cloud deployment environments but also available to on-premise deployments. Vaidio is responsible for providing this support.

5.2 Key Component Backup and Restore Service Levels

Description	Hours of Service	Backup Requirement	Service Level
Vaidio K8s and Cloud Platform	Continuous	Weekly full backup Daily differential /	Critical continuous service level to support overall SLA



Database system & data volume (including Configuration file)		incremental Monthly active Three years monthly archive	of 99%
Off-Site Storage	Continuous	Storage of electronic media by third party	As per SLA

6. Standard Operating Procedures (SOP)

The following SOPs are the basis for all work flowing through the Vaidio Operations and IT Support team. They cross boundaries between services and tie together multiple necessary activities to deliver seamless services to End-user Customers. These SOPs are not documented as services but are the basis for delivering those services.

When any issue arises that requires information or support from Vaidio, the End-user Customer is responsible for submitting a formal written request for service in the form of a ticket in the Support Portal: vaidio.myportallogin.com/.

For first-time users of Vaidio's Support Portal and ticketing system, instructions are as follow:

1. Register at vaidio.com/support (*skip this step if you have been in contact with Vaidio via email*)
2. Visit Vaidio **Support Portal**: vaidio.myportallogin.com
 - a. **SIGN IN** using Google or Microsoft if either is the provider of your business email account in Step 1 (*most common*), **OR**
 - b. **SIGN UP** using the same email address as that in step 1 (*You only need to do this the first time logging into the Support Portal*)
 - i. Select a password
 - ii. Check your inbox for an email from DoNotReply@connectwise.com titled "**Activate your ConnectWise account login**" with the link to validate your email address
 - iii. Go to vaidio.myportallogin.com, **Sign In** using the email and password in Step 2.i.
 - c. If you see the message "Request Permission to the Portal," return to Step 1
3. Start using the Support Portal by selecting Submit a Ticket

ADDENDUM
CYBERSECURITY AND INFORMATION SECURITY POLICIES AND OPERATIONS OF IRONYUN

1. IronYun VP of Operations & IT is responsible for the cybersecurity & information security of IronYun operations. His/her duties include but are not limited to:
 - Facilitate the confidentiality, integrity, and availability of data
 - Reduce the risk of security incidents, including cyberattacks and phishing attempts
 - Execute security programs across the organization
2. Device policy:
 - 2.1. BYOD policy is allowed, where the employees are held responsible for protecting the security of all data and communications as subjected to NDAs between the employees and IronYun, and between IronYun and partners/customers.
 - 2.2. Google Mobile & endpoints management and Google Security Checkup are used to manage company-issued devices.
 - 2.3. Each IronYun employee with remote access to the local environment and application is provided with a secured account, and the system logs the login of the accounts.
 - 2.4. Software installation for Vaidio design, production, training and testing is only allowed on company servers in the local environment.
 - 2.5. Only the teams responsible for a certain set of tasks have user access to the servers/software for that set of tasks.
 - 2.6. Bitlocker/Innodisk Hardware-based AES Encrypted Storage is used for device encryption.
 - 2.7. HiNet enterprise information security service is used for malware protection. The activities performed include, but are not limited to:
 - DDoS Protection
 - Virus Blocking
 - Intrusion Detection & Prevention
 - Malicious website blocking
 - 2.8. Lockout policy:
 - Server hardware logon will lock out for 30 seconds after three failed attempts with a wrong IPMI password.
 - The VPN account will be locked out after five failed attempts of Array VPN login.
 - Vaidio login will be locked out for at least 1-3 minutes if a wrong-password DDoS attack is detected.
 - 2.9. All mobile and computing devices that connect to the internal network must comply with the [Minimum Access Policy](#) (page 20)
 - 2.10. IronYun employees shall avoid downloading any data and information of and/or about IronYun and IronYun's customers from IronYun's secured data-sharing platform to personal devices unless absolutely necessary (such as presentation materials for offline events)

- 2.11. IronYun employees shall remove all IronYun's and IronYun's customer's information and data from personal devices as soon as the activity that requires the download is completed, so that such information cannot be recovered
3. The following devices & measures are used for the External Devices or Remote Access security:
 - FW - Palo alto PA-3020 / FortiGate 100D
 - VPN - Server Array Networks / MotionPro Clients
 - AWS VPN : AWS Virtual Private Network
 - AWS Client VPN
 - AWS Site-to-Site VPN
 - MFA:
 - Google 2-Step Verification / Authenticator / SMS
 - Vasco IDENTIKEY
 - Hubspot 2-Step Authentication
4. Information Security Awareness, Education and Training:
 - 4.1. IronYun provides regular information security training to all employees
 - 4.2. All IronYun employees are aware of and use security measures to avoid phishing campaigns
 - 4.3. IronYun provides regular information security training to the individuals responsible for management
 - 4.4. IronYun periodically checks the actual status of compliance with information security rules, by requesting all employees to perform self-inspection checks. The designated management personnel oversees the improvement of any nonconformities
 - 4.5. IronYun has a confidentiality section in the work rules or other regulations and obtains a commitment to confidentiality from employees
5. Asset management policy:
 - 5.1. Asset Management Policy is to establish the rules for the control of hardware, software, applications, and information used by IronYun.
 - 5.2. All hardware, software, and applications must be approved, inventoried, and purchased by IronYun OPIT.
 - 5.3. Software used by IronYun employees, contractors, and/or other approved third parties working on behalf of IronYun must be properly licensed.
 - 5.4. Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.

- 5.5. The use of cloud computing applications must be done in compliance with all laws and regulations concerning the information involved, e.g., personally identifiable information, protected health information, corporate financial data, etc.
 - 5.6. Two-factor authentication is required for external cloud computing applications with access to any confidential information for which IronYun has a custodial responsibility unless a waiver/exception form is formally approved.
 - 5.7. Contracts with cloud computing application providers must address data retention, destruction, data ownership, and data custodian rights regarding stored IronYun data.
 - 5.8. Hardware, software, and application inventories must be maintained continually.
 - 5.9. A general inventory of information (data) must be mapped and maintained on an ongoing basis.
 - 5.10. All IronYun assets must be formally classified with ownership assigned.
 - 5.11. IronYun assets exceeding a set value, as determined by company or IT management, are not permitted to be removed from IronYun's physical premises without management approval.
 - 5.12. All IronYun physical assets exceeding a set value, as determined by management, must contain asset tags or a similar means of identifying the equipment as being owned by IronYun.
 - 5.13. Confidential information must be transported either by a designated IronYun employee or a courier approved by IT management.
 - 5.14. Upon termination of employment, contract, or agreement, all IronYun assets must be returned to IronYun management or leadership and documented accordingly.
6. Data classification policy - IronYun establishes a framework to classify data based on its sensitivity, value and criticality to the organization, so sensitive corporate and customer data can be appropriately secured .

Classes of data, determined by sensitivity	Data types	Security Level
Confidential	Product development data: IronYun's intellectual property, including all source codes and default models for all customers' use	Critical

Internal	IronYun organization data: including employee information, inventory information, accounting data, etc. Customer data: for model training and model/engine testing	
Public	Publicly available data used and processed by Vaidio to display in demos, such as data from Earthcam streams	High

7. Confidential management of information assets:

- IronYun regularly identifies and inventories sensitive information
- When reproducing or duplicating any confidential information in compliance with the relevant agreement, IronYun maintains the reproduced or duplicated confidential information in the same manner as the original
- IronYun manages confidential information separately from other information

7.2. Disposing of confidential information:

- In the case of electronic information, IronYun employees completely erase all confidential information stored on servers, personal computers, portable devices, and recording media
- In the case of information on paper (documents, drawings, etc.), IronYun employees properly shred, dissolve, or incinerate it
- In the case of embodiments (molds, prototypes, etc.), ironYun employees destroy it so that no confidential information can be discerned

7.3. Physical Management:

- IronYun has physical measures in place to restrict entry of unauthorized individuals to locations (premises, buildings, rooms) where confidential information is handled, such as access cards, badge locks, face recognition system
- Person responsible for management within their department allows only those who need to know confidential information in the course of their work to enter the area where such information is handled
- IronYun strategically locates and installs critical systems, equipment, and wiring related to confidential information to avoid damage from natural disasters such as earthquakes and man-made accidents such as tripping over cables
- IronYun ensures that paper information (documents, drawings, etc.) and embodiments (molds, prototypes, etc.) can only be accessed by those who need to know the information for business purposes and takes measures to prevent theft

7.4. Management of Information System User IDs:

- IronYun has established the following rules for managing user IDs for information systems:

- Prohibit information system users to share IDs with other users
 - Establish procedures for issuing and approving user IDs for information systems
 - Immediately delete IDs of retirees, transferees, and others who are no longer involved in related work, as well as temporary user IDs and other IDs that are no longer needed
 - Periodically check that there are no unmanaged IDs
- 7.5. IronYun prohibits the installation and use of file exchange software (software with a high risk of information leakage) and regularly checks for the installation and use of such software
- 7.6. IronYun prohibits the transmission or sharing of confidential information via free email services (Yahoo! Mail, etc.) or data sharing services (Google docs, etc.)
- 8. Data destruction policy: On termination of the provision of Personal Data processing services, IronYun shall be under obligation to delete all Personal Data processed on behalf of Partner and certify to Partner that it has done so unless Union or Member State law or other law to which IronYun is subject requires further storage of the Personal Data by IronYun.
- 9. Access Management Policy:
 - [Minimum Access Policy](#) (page 20)
 - [Password policy](#) (page 22)
- 10. Cryptographic management policy: a) user passwords are encrypted (PBKDF2); b) SSL/TLS (AES 256) is used to protect the data transmission; c) user data and system data encryption rely on SSD encryption as described in Section 2.6.
- 11. Physical and environmental security policy: IronYun's VP of Operations (or designee) monitors a wide variety of possible risks that may affect IronYun. These risks include utility outages, building safety systems, security issues, weather, seismic activity, and market and finance volatilities. IronYun also has a proactive building maintenance program that is intended to prevent utility and equipment failures and malfunctions that could lead to a crisis. In addition, IronYun's staff conducts a wide variety of routine inspections of work areas and conditions to ensure that safety hazards are identified and corrected in a timely manner.
- 12. Endpoint security policy:
 - 11.1 Measures taken to maintain and update endpoint security solutions:
 - Regularly checking to see whether the endpoint security solution is up to date by routinely updating the program with the newest security patches and bug fixes
 - Looking for any shady activity on endpoints involving atypical account logins or sudden updates or downloads
 - Conducting routine malware and other malicious software checks on endpoints
 - Informing IronYun staff about the best internet security and safety practices, including employing solid passwords and eliminating phishing emails

- Using a solid firewall to stop malicious connections from getting to the endpoints
- Setting up automatic security updates
- Using two-factor authentication

11.2 Measures taken to handle endpoint security incidents and breaches:

- Identify and isolate the affected endpoint
- Assess the damage
- Contain the incident or breach
- Investigate the incident or breach
- Remediate the issue
- Communicate with stakeholders
- Learn from the incident or breach

11.3 Measures taken to handle endpoint security compliance requirements:

- Implement access control measures
- Monitor and audit endpoints
- Encrypt data
- Patch management
- Use application whitelisting
- Backup data

11.4 Measures taken to handle endpoint security in a remote work environment:

- Establish Security Protocols
- Monitor and Control Access
- Use a Virtual Private Network (VPN)
- Implement Firewall and Antivirus Software
- Educate Employees
- Restrict Unauthorized Access
- Monitor Network Activity

11.5 Measures taken to handle endpoint security for mobile devices:

- Verifying that all mobile devices' operating systems and security updates are current to reduce the possibility of security vulnerabilities.
- Using a mobile device management (MDM) service to manage a mobile device, which enables one to remotely modify device settings and impose security regulations such as encryption and password restrictions.
- Requiring IronYun employees to turn on two-factor authentication on their gadgets to prevent illegal access to gadgets.
- Ensuring that any private information saved to the gadget is encrypted.
- Establishing a security policy for mobile applications to ensure that any programs downloaded and installed on the device are safe and current.

13. Backup policy:

- 13.1. Full and incremental backups protect and preserve corporate network information and should be performed on a regular basis for system logs and technical documents that are not easily replaced, have a high replacement cost, or are considered critical.
- 13.2. Backup media should be stored in a secure, geographically separate location from the original and isolated from environmental hazards.
- 13.3. Backup network components, cabling and connectors, power supplies, spare parts and relevant documentation should be stored in a secure area on-site as well as at other corporate locations.
- 13.4. Data and document retention policies are established to specify what records must be retained and for how long.
- 13.5. All departments are responsible for specifying their data management, data retention, data destruction and overall records management requirements.
- 13.6. See the below sample for backup policies and backup plan

Service	Service Owner	Priority	Description	Service Location	OS or App	Data Size	Backup Frequency	Repository	Responsible for backup	Status
BITBUCKET	Ying-Chu	High	Source Code	bitbucket.org/ironyun	SaaS	<200GB	Every Release Manually	Download and store in NAS://RD	Ying-Chu	
JIRA	Same	Medium	Development	Ironyun.atlassian.net	SaaS	<200GB	Bi-Monthly Manually	Download and store in NAS://RD	Ying-Chu	
AI Training	Patrick	High	Training data set	Patrick's PC	MAC OS	1TB	Weekly Manually	Backup to AI-4 training machine	Patrick	
Jenkins	Same	Medium	Build/Rep server	172.16.15.10 172.16.15.109	Ubuntu	10TB	Daily-Auto	Download and store in NAS://RD	Same	
Figma	Karen	High	UI/UE Specs.	www.figma.com	SaaS	<30GB	Every Release Manually	Download and store in NAS://RD	Karen	
Google drive Eng. folder	Karen	High	Eng. Data	Google Cloud	SaaS	<100GB	Daily-Auto	Download and store in NAS://RD	Karen	
ERP	Sonia	High	Sunlike ERP	172.16.15.55	WinSrv	1.26GB/day	Auto-Daily/Manual-Monthly	1. Unlike general BF daily(Sonia) 2. Sync copy to BS via script daily	Leo	

14. Log management policy: IronYun's log management policy establishes processes to ensure that all relevant system logs are accessible and consistently monitored. All production systems within IronYun shall record and retain audit-logging information that includes the following information:
 - 14.1. Vaidio logs:
 - System log: analyze specific trends or record the data-based events/actions of the Vaidio system environment network. Three log types: INFO, WARN, ERROR
 - Diagnostic log: encrypted log of hardware errors, processing consumption, analytic/alert/connection errors, failed login attempt from the IP address of the computer trying to access Vaidio
 - Audit trail: successful user login/logout, time and user actions in the entire Vaidio system (such as camera activation/modification)
 - 14.2. IronYun operations logs:
 - Each team has a logging system to keep track of activities, inventory, tasks, etc.
 - 14.3. IronYun support portal:
 - Ticketing system for technical support and information; central log of support activities between customers and IronYun

15. Vulnerability and Patch Management process:

Vaidio undergoes professional tests and vulnerability scans with each release to ensure software security and stability, while also ensuring customer satisfaction. For system security scans, tools like Trivy, Snyk, and Nessus are used. Please refer to the latest [Vaidio Scan Report](#) for more information.

16. Network security policy:

- 16.1. Users are permitted to use only those network addresses assigned to them by Ironyun's IT Department OPIT.
- 16.2. All remote access to IronYun will either be through a secure VPN connection on a IronYun owned device that has up-to-date anti-virus software, or on approved mobile devices
- 16.3. Remote users may connect to IronYun Information Systems using only protocols approved by IT.
- 16.4. Users inside the IronYun firewall may not be connected to the IronYun network at the same time a remote connection is used to an external network.
- 16.5. Users must not extend or re-transmit network services in any way. A user must not install a router, switch, hub, or wireless access point to the IronYun network without IronYun IT approval.
- 16.6. Users must not install network hardware or software that provides network services without IronYun IT approval. Non-IronYun computer systems that require network connectivity must be approved by IronYun IT.
- 16.7. Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, IronYun users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the IronYun network infrastructure. Only the IT Department is permitted to perform these actions.

17. Secure Software Development Lifecycle (SSDLC) policy: IronYun's Software Development Life Cycle (SDLC) includes the following phases:

- Requirements Analysis
- Architecture and Design
- Testing
- Deployment/Implementation
- Operations/Maintenance

Paid secured source code control service (bitbucket) is used to manage the source code. Code committed by developers must be reviewed before merging to the source tree. An on-site CI/CD process (Jenkins) is built, which automatically pulls the source code, builds the software

binary and performs a security scan and coding style scan using Trivy, Snyk, Nessus, and Fortify. The CI/CD process also performs software feature tests and automatically generates reports. In parallel, IronYun has a dedicated QA team to perform manual software feature testing and create test cases for test automatization. A complete test report, which includes a functional test report and a security test report, is generated and reviewed for every release. A paid secured bug tracking service (JIRA) is adopted to track the discovered issues, and a paid secured test case management service (Zephyr) is adopted to track all test cases created.

18. Secure coding training to developers: IronYun developers follow the most up-to-date best practices in coding to maximize code security. All codes are tested for vulnerabilities during and after development using the software tools mentioned in section 16. All security holes and potential bugs that may impact the security of the software codes are reviewed for every release, and critical/major risks will be addressed as soon as possible (including IronYun's product lines and third-party products that IronYun uses for development).
19. The last penetration testing performed by an external third-party company was completed on August 2023 by an end-user customer (a large multinational enterprise, whose name IronYun does not have permission to reveal due to the mutual NDA in effect).
20. Third-party/subcontractor management policy that includes third-party security checks deployed:
 - 20.1. IronYun Third-Party Management Policy:
 - IronYun makes every effort to assure all 3rd-party organizations are compliant and do not compromise the integrity, security, and privacy of IronYun or IronYun Customer data.
 - 3rd Parties include Customers, Partners, Subcontractors, and Contracted Developers.
 - 20.2. Policies to Assure 3rd Parties Support Organizational Compliance
 - The following are required before 3rd parties are granted access to any IronYun systems:
 - Due diligence with the 3rd party;
 - Controls implemented to maintain compliance;
 - Written agreements, with appropriate security requirements, are executed.
 - All connections and data in transit between the IronYun Platform and 3rd parties are encrypted end to end.
 - Access granted to external parties is limited to the minimum necessary and granted only for the duration required.
 - A standard business associate agreement with Customers and Partners is defined and includes the required security controls in accordance with the organization's security policies. Additionally, responsibility is assigned in these agreements.

- IronYun has Service Level Agreements (SLAs) with Subcontractors with an agreed service arrangement addressing liability, service definitions, security controls, and aspects of service management.
- IronYun utilizes monitoring tools to regularly evaluate Subcontractors against relevant SLAs.
- Third parties are unable to make changes to any IronYun infrastructure without explicit permission from IronYun. Additionally, no IronYun Customers or Partners have access outside of their own environment, meaning they cannot access, modify, or delete anything related to other 3rd parties.
- Whenever outsourced development is utilized by IronYun, all changes to production systems will be approved and implemented by IronYun workforce members only. All outsourced development requires a formal contract with IronYun.
- IronYun maintains and annually reviews a list of all current Partners and subcontractors.
- IronYun assesses the security requirements and compliance considerations with all Partners and Subcontracts.
- Regular review is conducted as required by SLAs to assure security and compliance. These reviews include reports, audit trails, security events, operational issues, failures and disruptions, and identified issues are investigated and resolved in a reasonable and timely manner.
- Any changes to Partner and Subcontractor services and systems are reviewed before implementation.
- For all partners, IronYun reviews activity annually to assure that partners are in line with SLAs in contracts with IronYun.

20.3. Inventory and classification of outsourced products & services:

- If a product or service will be outsourced, both the due diligence during the selection process and the ongoing oversight of the selected vendor will be based on IronYun's assessment of the importance or criticality of the outsourced product or service, but all vendors will have some level of ongoing oversight.
- An inventory of third-party service providers shall be maintained, the inventory shall include:
 - Vendor risk level;
 - Types of data shared with the third party, including data classification;
 - Brief description of services; and
 - Significant controls in place.
- Vendor risk level assessment will be based on the following considerations:
 - A product/service will be designated "critical" if:
 - The vendor will be performing processing required for daily activities;
 - The vendor has access to Restricted/Sensitive information;
 - The service is significant to IronYun's strategic plans; and
 - executive management designates it as such.

- A product/service will be designated "major" if:
 - The vendor will perform any processing for IronYun;
 - The product is important to IronYun's competitive posture; and
 - Executive management designates it as such.
- A product/service will be designated "low" if:
 - • The service is minimal to IronYun's strategic plans;
 - • The vendor's own reputation does not harm IronYun's reputation; and
 - • Executive management designates it as such.

20.4. **Third Party Contracts.** Formal contracts that address the relevant security and privacy requirements must be in place for all third parties that process, store, or transmit confidential data or provide critical services. The following must be included in all such contracts:

- Contracts will acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits;
- Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party;
- Contracts identify the recourse available to IronYun should the third party fail to meet defined security requirements;
- Contracts establish responsibilities for responding to direct and indirect security incidents including timing as defined by service-level agreements (SLAs);
- Contracts specify the security requirements for the return or destruction of data upon contract termination;
- Responsibilities for managing devices (e.g., firewalls, routers) that secure connections with third parties are formally documented in the contract; and
- Contracts stipulate geographic limits on where data can be stored or transmitted.

20.5. **Third-Party Review.** In all cases where IronYun's sensitive, critical services or data are provided to a third-party service provider, IronYun must review the service provider's internal control structure to ensure compatibility with IronYun Information Security requirements. The request and the results of the review should be provided to the Management Team. Once the relationship is established, an ongoing review of the service provider's internal controls structure is required on at least an annual basis. The evaluation of a third party may include the following items (if applicable):

- Audited financial statements, annual reports, SEC filings, and other available financial information;
- Significance of the proposed contract on the third-party's financial condition;
- Experience and ability in implementing and monitoring the proposed activity;
- Cost analysis comparing the Vendor's offering to other methods of performing the service, including the use of the other potential vendors and performing the service in-house.

- Business reputation of the Vendor (including reference checks with current customers);
- Qualifications and experience of Vendor's principals;
- Strategies and goals, including service philosophies, quality initiatives, efficiency improvements; and employment policies;
- Existence of any significant complaints or litigation, or regulatory actions against the Vendor;
- Ability to perform the proposed functions using current systems or the need to make additional investment;
- Use of other parties or subcontractors by the Vendor;
- Scope of internal controls, systems and data security, privacy protections and audit coverage;
- Business continuity and disaster recovery plans;
- Adequacy of management information systems;
- Insurance coverage.

21. Security Incident Management policy:

21.1. Security incident:

- Refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. Incidents can include, but are not limited to, unauthorized access, malicious code, network probes, and denial of service attacks.
- Security Incident Management at IronYun is necessary to detect security incidents, determine the magnitude of the threat presented by these incidents, respond to these incidents, and if required, notify IronYun members of the breach.

21.2. Program Organization:

- Computer Emergency Response Plans – IronYun management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical computer and communication systems in the event of an interruption or degradation of service. For example, Charter connectivity is interrupted or an isolated malware discovery.
- Incident Response Plan Contents – The IronYun incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise, including notification of relevant external partners. Specific areas covered in the plan include:
 - Specific incident response procedures
 - Business recovery and continuity procedures
 - Data backup processes
 - Analysis of legal requirements for reporting compromises
 - Identification and coverage for all critical system components
 - Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers

- Incident Response Testing – at least once every year, the IT Department must utilize simulated incidents to mobilize and test the adequacy of response. Where appropriate, tests will be integrated with testing of related plans (Business Continuity Plan, Disaster Recovery Plan, etc.) where such plans exist. The results of these tests will be documented and shared with key stakeholders.
- Incident Response and Recovery – A security incident response capability will be developed and implemented for all information systems that house or access IronYun controlled information. The incident response capability will include a defined plan and will address the seven stages of incident response:
 - Preparation
 - Detection
 - Analysis
 - Containment
 - Eradication
 - Recovery
 - Post-Incident Activity
- To facilitate incident response operations, responsibility for incident handling operations will be assigned to an incident response team. If an incident occurs, the members of this team will be charged with executing the incident response plan. To ensure that the team is fully prepared for its responsibilities, all team members will be trained in incident response operations on an annual basis.
- Incident response plans will be reviewed and, where applicable, revised on an annual basis. The reviews will be based upon the documented results of previously conducted tests or live executions of the incident response plan. Upon completion of plan revision, updated plans will be distributed to key stakeholders.
- Intrusion Response Procedures – The IT Department must document and periodically revise the Incident Response Plan with intrusion response procedures. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.
- Malicious Code Remediation – Steps followed will vary based on scope and severity of a malicious code incident as determined by Information Security Management. They may include but are not limited to: malware removal with one or more tools, data quarantine, permanent data deletion, hard drive wiping, or hard drive/media destruction.
- Data Breach Management – IronYun management should prepare, test, and annually update the Incident Response Plan that addresses policies

and procedures for responding in the event of a breach of sensitive customer data.

- Incident Response Plan Evolution – The Incident Response Plan must be updated to reflect the lessons learned from actual incidents. The Incident Response Plan must be updated to reflect developments in the industry.

21.3. Program Communication:

- Reporting to Third Parties – Unless required by law or regulation to report information security violations to external authorities, senior management, in conjunction with legal representatives, the Security Officer, and the VP of IT must weigh the pros and cons of external disclosure before reporting these violations.
 - If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, these third parties must be immediately informed about the situation.
 - If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its Owner and the Security Officer must be notified immediately.
- Display of Incident Reporting Contact Information – IronYun contact information and procedures for reporting information security incidents must be prominently displayed in public communication mediums such as bulletin boards, break rooms, newsletters, and the intranet.
- Member Notification – The notification will be conducted and overseen by IronYun’s Director of Risk Management. The notification should contain, at a minimum, the following elements:
 - Recommendations for the member to protect him/herself
 - Contact information for the Federal Trade Commission
 - Contact information for the credit bureaus

22. IronYun conducts quarterly internal audits of information security prior to each product release and as needed in the event of security issues of related products by partner companies and vendors. The VP of Operations or his designee will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.