OperationsCommander: Security Whitepaper

As do many, we take security very seriously!

We understand that the data we have been entrusted with is data which our clients have also been entrusted with. We always ensure that we go well above and beyond the requirements and standards for safe secure storage and handling of all data. This whitepaper outlines in details some of the lengths which we go to ensure business continuity and respect for entrusted data.

This whitepaper was reviewed May 2022

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

Executive Summary

OperationsCommander (OPS-COM) is a cloud-based parking and security management platform. This platform has been developed in-house for over 15 years.

Tomahawk Technologies Inc. is committed to maintaining a high level of information security, and its key priority is protecting customer information, and carefully maintaining the information security of OPS-COM. This Security Whitepaper gives an overview of the OPS-COM security features.

OPS-COM is PCI SAQ D-SP 3.2.1 certified and is audited quarterly by a third-party to maintain this certification. Risk analysis forms the foundation of our security program.

Risk assessments are periodically performed, and security is regularly discussed in weekly team meetings. Our security processes, roles, and responsibilities are clear and well defined. Everyone is aware of our responsibilities and obligations when protecting our client's data.

We review our policies annually and ensure that all employees sign-off on them. OPS-COM is developed and maintained by inspired, skilled personnel who are committed to maintaining a high level of online security. OPS-COM has been designed to meet customers' strict security requirements and industry best practices.

OPS-COM has a solid and secure foundation that is based on widely used security methods and protocols. It has been designed to protect data both in transit and at rest to ensure its confidentiality, integrity, and availability. Strict access control allows only authorized users to access the data.

Operation and maintenance of OPS-COM follows documented processes. Continuous monitoring of information security and system performance ensures that all deviations and incidents can be responded to in a timely manner by trained and competent personnel in accordance with the incident response process.

This document is designed to answer all your questions regarding the security and design of both OPS-COM and our supporting systems.

92 Bridge Street ● Carleton Place ● ON ● K7C 2V3
Toll Free: 855.410.4141 ● Fax: 613.257.4141

General OPS-COM Information	
What browsers are supported?	OperationsCommander recognizes that our users may user various Internet Browsers when working with our system. We aim for all visitors to have the best possible experience while using OPS-COM, however, we do recognize that it is impossible to develop applications that work identically, efficiently, and effectively on all web browsers. We make best efforts to support the latest versions of • Internet Explorer • Safari • Chrome • Firefox
Is OPS-COM mobile friendly?	The site supports browsing with mobile or tablet devices. Content is sized and displayed based on the screen resolution and other display attributes of your device. Our violations app is specific to Android devices. Not all tablets or mobile devices are supported for use with "OPS-COM for Android" as processing power and camera functions may vary. OPS-COM supports version 7 and higher of the Android operating system.
Who owns OPS-COM?	OPS-COM owned by Tomahawk Technologies Inc., a privately owned, Canadian company. 92 Bridge St. Carleton Place, ON Canada 855-410-4141
What laws govern the contractual agreement as it relates to the licensing arrangement?	The laws of the province of Ontario

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

What is your Privacy Policy and how is it implemented?	Appendix B in our Contract outlines our privacy policies. All employees review and acknowledge our Privacy and Security policies annually. All employees sign confidentiality agreements.
Product Lifecycle	
Describe your coding practices and how you security test your applications.	We use: • Peer code reviews • QA & testing by junior developers and non-developer staff • Third-party scanning • Web application vulnerability testing • Automated testing
How often are new versions of OPS-COM released? Who performs these upgrades? Are they disruptive to customers? Are they disruptive to the service availability?	We do monthly updates with any potential changes being released to a preview (production mirror site) one week before it is moved to client's production code. System Administrators work with in-house Developers to release these code changes. These releases are transparent to clients and rarely, if ever, disrupt service. Notifications are sent out prior to the release to inform the client that the release is coming and should be tested and reviewed based on client workflow. Release notes and documentation are available prior to release to preview. Critical hot fixes are occasionally released to production systems as warranted. With less than 1 hour lost to down time in the past 12 months, we are averaging an up time better than 99.99%

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

Are your systems and applications scanned for vulnerabilities [that are remediated] prior to new releases?	Product testing involves many different levels of security scan and known vulnerability testing.

Incident Response Plan	
Have you had a significant breach in the last 5 years?	No
What happens if there is a breach or a data security incident?	If there is an incident, the client would be notified with all pertinent details. Depending on the severity of the issue, the system would be disconnected from the network and a snapshot of the system state and hard drive would be taken (all systems are VM's) Our contracts state the following: If the Service Provider anticipates a breach of privacy or becomes aware of a breach relating to the personal information received, collected, retained, or stored by the Service Provider in the course of performing the Services, the Service Provider must immediately notify the Customer in writing of the following, to the extent known: • the nature of the information that was breached (type and date of the information, name(s) of the person(s) whose information is affected); • when the breach occurred; • how the breach occurred; • who was responsible for the breach; • what steps the Service Provider has taken to mitigate the matter; and • what measures the Service Provider has taken to prevent re-occurrence

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

What are the qualifications of your incident response staff?	Our development/technical staff have been working with the software application and servers for many years. Currently we employ: • 2 senior developers with application and system knowledge • 2 junior developers with limited application and system knowledge • 1 system administrator with advanced knowledge in regard to setup, firewall, web server, SQL, and VM platforms All developers and system administrators are required to participate in our security awareness program.
Processes & Policies	
What is your change control process as it relates to OPS-COM?	We assess new technologies regularly. Through small office lunch-and-learn sessions, and meetings, we discuss future initiatives. At this time much of our software (functional) changes are driven by client requests and therefore managed as projects. Internally we also investigate opportunities to integrate technical improvements with every project.
Does the Service Provider have formal written Information Security Policies?	Yes, we have 18 PCI compliant policies and an additional 3 Security policies that are required to protect our data and that of our clients while maintaining a high standard of data security.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

Describe your information security (INFOSEC) organizational structure and your policies.	We are a small office of ~10 staff, with 1 server administrator and 2 senior developers. Any tech issues flow through these staff members. The business owner is a key architect to the application and one of the senior developers. Security and process are regular points for discussion at team meetings and all employees have knowledge of PCI requirements for data security. Polices are documented and reviewed regularly.

Third-Party Compliance

Are you SOC 2 compliant?	No, not at this time.
Are you PCI compliant?	Yes, we are PCI DSS 3.2.1 compliant. We are assessed annually by a 3rd party to ensure we maintain compliance. Our Attestation of Compliance, SAQ D-SP is available upon request
Do you have an assessment on file with the Higher Education Community Vendor Assessment Tool (HECVAT)?	Yes, we have completed the Lite questionnaire.
Have you undergone a SSAE 18 audit?	No, however, we follow all the principles of PIPEDA (Personal Information Protection and Electronic Documents Act). We are also PCI (Payment Card Industry) certified, which relates to the storage and transmission of personal and financial data.

Disaster Recovery

Do you have a disaster recovery process?	We have a Disaster Recovery Plan that is tested every 3 months. Backups are performed using external hard drives and are kept for 7 years. Backups are located at the data center and head office.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?	Recently due to COVID-19 all operations were transitioned to remote or a telework environment with no issues.

Data Model and Data Security	
Describe your application's architecture and tiered design	Our Web servers are publicly accessible; however, our SQL servers are not. SQL servers are backed up daily and mirrored to a secondary system. All data is stored to iSCSI RAID devices which are on a separate network. The system is multi-tenant, as an example iSCSI LUN's are separated and on network accessible only to VM hosts.
How do you protect user authentication information?	Usernames and passwords are used and are stored to the SQL server. Passwords are encrypted with a minimum Blowfish 64 bit key for legacy systems and for OPS-COM systems that use Android or PHP rijndael-128 is used. All passwords are hashed for one-way hashing. IP filtering is also employed. OPS-COM allows for password aging and complexity requirements to be enforced. Client files can be accessed by system administrators and senior developer's only, and only on an as-required basis. All access is logged.
Is Data protected "at rest" and "in motion"?	All sensitive data is encrypted in-transit and at-rest. Data in Motion: all transfers are logged; all transfers are encrypted. Data at Rest: is secured using Column level encryption within the database with a minimum 128-bit encryption in all areas.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

How is data backed up, stored, and protected?	Client user files are backed up and held for 7 years on external hard drives unless requested to be destroyed earlier. These hard drives are always held in a secure location. External Hard drives are the only removable media we use to store client data. We do not store client media on desktops, laptops, or BYODs. Client data is occasionally stored on systems owned and operated by a third-party but only as required for proper system functionality and in a very limited capacity. For example, Digital Ocean is used to store/host ticket images, no other data is hosted with third-party services Our backup procedures are multi-tiered since data is the single most important detail for business continuity. • all systems run on RAID-10 storage devices • all servers utilize iSCSI storage link to RAID-10 hardware • all SQL services replicate all data to a designated data mirror server or data cluster (dependent on service level) • all VM's are backed up (complete VM; OS & data snapshot) once per month and maintained for 3 months • all dynamic data (script + SQL) is backed up nightly and maintained indefinitely (or until contract termination) • single day backups are maintained for one week • weekly backups are maintained for two months • monthly backups are maintained for 7 years (or until contract termination) • emergency and data restore tests are performed regularly

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

	We maintain a separate data link specifically for storage traffic. This (SAN) network is physically disconnected from the main LAN (and WAN) network. All backups are stored at the co-location facility on a server that is designated solely for this purpose. On a rolling (nightly) schedule, backups are pushed to a removable device which is physically removed (quarterly) and stored in an offsite secure location Client data does exist on development, QA and preview environments. These environments are secured in the same fashion as production data. When disk media is destroyed Tomahawk uses Secure Erase as outlined by the U.S. National Institute of Standards and Technology (NIST) External backup drives not stored at the data center are retained at head office for long term storage (7 years). Physical security includes retinal scan (NOC), locked doors, keypads, alarm systems, motion sensors, and a locked safe. Access to external drives is limited to OPS-COM employees who explicitly require such access to provide disaster recovery and backup retrieval services.
Do backups containing institution data ever leave the institution's Data Zone, either physically or via network routing?	Offsite backups exist as a product of business continuity. These backups are secured and are accessible only to system administrators.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

Who has access to your data and who approves this access and are we notified?	Technical support personnel who require access to support clients or require access to perform job duties and responsibilities have access to client data. This may include programmers, system administrators, and client support staff. System administrators determine who requires such access based on requirements. We log our access to client data when we do either testing (upcoming releases for new functionality) or for support reasons.
Can employees access customer data remotely?	Yes, for support and service purposes and only key employees. Tomahawk staff logins are through VPN and access is based on role and controlled by LDAP rules. Application staff logins can be limited and filtered by IP address.
Who is considered the owner of client data stored in vendor or third-party Data Centers?	The client always owns their database of information on the system. We will provide a raw data dump in a SQL file format (or zip archive) for the client to use as required. There are small fees for creating and providing to the client the data file. We will not provide the architecture or road map of the data since that is considered proprietary information.
How do you segment and isolate our customer instance and data from other customer data?	Each customer instance has a separate database with separate login credentials.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

Describe the permissions granted to each role in your application/system?	OPS-COM can set up permissions for all roles. The Super User, (usually the department head) sets permissions for all levels. For example, counter staff could have permission to add/edit payments but not edit site configuration. A patrol officer could enter violations but not edit violation types. All permissions are set using the Edit Admin Users menu. This edit window is only accessible to the Super User and any others that the Super User grants "Edit Admin Users" permission to. Other permissions that are part of the table is the ability to limit where a user can log in from. IP restrictions can be implemented to a single computer, area, the whole site or completely open. The Super User can grant the ability to work from offsite locations. i.e., work from home or limited to a single area within a location. Multiple IP addresses can be specified. There are more than 75 permissions that can be set to fine tune any role. When the permissions are assigned, the assignee will only see what they can do. They will not be aware of restricted permissions.
Do you ever use client data for analysis? Is client data ever shared with 3rd parties?	No.
What are the acceptable data transmission methods to allow client data to be uploaded to the OPS-COM system?	Any traffic uploaded or downloaded to the service would be encrypted with Transport Layer Security (TLS). e.g. HTTPS (web/API) SFTP (secure FTP). Generally, data will use one of these protocols. In some cases, data will pass been SQL servers using encryption (utilizing TLS).
In what format will clients be provided their data if they are leaving OPS-COM?	The client always owns their database of information on the system. We will provide a raw data dump in a SQL file format (or zip archive) for the client to use as required. There are service fees for creating and providing the data file. We will not provide the architecture or road map of the data since that is considered proprietary information.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

Does the system provide data input validation and error messages?	Yes
Does the Vendor have a mobile application that can access the client's data/application? If so, please describe how the mobile application code is validated for security risks?	OPS-COM for Android pulls select pieces of data from the main database to identify and validate vehicles in the field. Any violations that are created are pushed to the server to be linked to a user's profile based on the vehicle details. All communication is performed over a secure SSL link.
Are audit logs available that include AT LEAST all of the following: login, logout, actions performed, and source IP address?	Yes
System & Network Security	
What is your system availability notification process?	System availability is monitored with monitoring software. Logs are monitored for errors and anomalies. All technical staff are notified of any outages, 24/7. Clients are notified of outages if they are not rectified within 1 hour.
Who has access to these systems and how do they authenticate	System administrator and senior developers have access, and they authenticate through VPNs using Microsoft Active Directory accounts with proper permissions. Passwords are managed through BitWarden. All access, including administrative accounts, is controlled and logged (i.e., firewalls, file system permissions, ACLs, database table permissions, packet logs, etc.)

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

What is your patch management process?
 	
What is the patching protocol for back-end infrastructure? How often are critical hotfixes to server OS, database and other components installed?
	System and Operating System:
	
	• Software (Kaspersky) monitors available system patches. The software reports software as well as operating system updates which are available.
	• On a regular basis firewall and network devices are updated with new firmware.
	• All server/system updates are tracked using logging tools.
	• Patches are rolled to staging systems, when possible, to reduce system failure risks.
	
	Software releases:
	
	• OperationsCommander maintains several systems including development, testing/preview, and production
	  ○ Development systems exist for development
	  ○ Testing/staging/preview systems exist to allow for testing of new patches and software updates
	  ○ Testing/staging/preview systems also exist for testing and training to avoid these actions on production systems
	  ○ Software is rolled to production with messages and release notes to clients about the updates
	
	Weekly, most updates are done automatically (such as OS). In some cases where additional testing and precautions are required before an update, the patch maybe delayed by a few days.

Describe your vulnerability management and notification process.	Third party security audits, email notifications of errors (sometimes security related). Quarterly we are scanned for system vulnerabilities by a 3rd party.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

How is your production network segmented from your corporate, QA, and development environments?	There are completely different servers, code, and databases. Testing/quality (QA) and development (dev) servers are also located in a different physical location. Non-production servers (preview, QA, and dev) are also sandboxed as to not allow database connections to production systems, emails are blocked from being sent out, etc. No matter what is done in a non-production system, the production systems won't be affected.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

Describe your systems High Availability features	To offer high availability at the operating system level, we use Citrix XenServer technology to provide a virtualized server environment. This allows us to maintain 6 physical servers (running numerous server VM's) which can act as DOM0 (server master) at any point in time. In a case where one VM is running away with CPU or eating up memory, the other VM's will be transitioned automatically to a designated secondary, with no noticeable adverse effect. If a physical server requires maintenance a secondary server can manually be designated to handle the load and ensure that the virtual server(s) and exposed services are not affected. In the case of web services, our website hosting servers have automatic load balancing in place between multiple servers. If one of the web servers is inaccessible, such as in the case of Windows updates or a reboot, our system will automatically stop directing web traffic to the inaccessible web server and start directing web traffic to the other available servers. In the case of SQL services, our SQL database servers are mirrored to sister servers (dependent on service level) which fail-over automatically under similar conditions. Whether due to maintenance or increased load, this allows our technical team to take a server offline at any time with no affect to client services. At the network layer, we employ a backup firewall device which would take on the role of master in the event of a physical firewall failure. All sites that provide service to our clients have redundant internet links to provide for high availability. There are 7 different upstream providers and several different network links that pass traffic through the network operation center for redundancy.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

Do you have a vulnerability management and penetration testing program?	SecurityMetrics does our vulnerability scanning. These scans identify top risks such as improperly configured firewalls, malware hazards, and remote access vulnerabilities.
What type of firewalls do you use? Are you using Next Gen Firewalls and IPS to secure your Data center customers from the internet? If you are using a third-party hosting provider such as Azure or AWS, are you operating any advanced threat detection services through that vendor? Are you utilizing a web application firewall (WAF) and/or a stateful packet inspection (SPI) firewall?	Firewalls used: • NOC: SonicWall NSA 2400 MX • Office: SonicWall TZ 205 Yes, deep pack inspection (DPI), network monitoring, and application firewall are all used by our firewalls. We also utilize Digital Ocean firewalls to limit access to data and SQL cluster. This setup includes strong ingress and egress rules to limit outgoing and filter incoming data packets.
Do you monitor for intrusions on a 24x7x365 basis?	Systems are monitored and based on parameters will notify system administrators through SMS test messages.
Do you have a documented policy for firewall change requests?	Yes, all firewall access is logged and tracked.
How are system/network monitoring, logging and alerting setup?	• Automatic network monitoring software (HostMonitor). email notifications, text notifications, status display screens. • PaperTrail - cloud logging • Sentry.io - error reporting related to code anomalies
Are systems that support this service managed via a separate management network?	Yes, via internal LAN and VPN access limited by IP address.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

How do you safeguard against virus and malicious code?	We use Kaspersky software on all systems to help ensure virus/malware clean systems. This same software offers firewall and malicious process monitoring. A central dashboard offers daily reports of issues or items of importance (i.e.. Windows and application software update availability) No software is installed on servers once in production, with minor exceptions. Servers are never used as desktop systems.
What are your capacity management practices?	• systems are load balanced using nginx • resources are monitored through VM management tools
Is wireless networking used in your organization	Yes, wireless networking is used at the OperationsCommander head office in Carleton Place. • Corporate WIFI access is limited by device MAC address. • Public WIFI is available for staff cell phones, laptops, and other devices. Public WIFI is separate from the corporate network.
What are you currently performing in terms of build hardening?	System hardening is based on our policy System Lockdown Policy. This policy is designed to minimize risk to organizational resources and data by establishing a process for increasing the security of servers and workstations by stopping unneeded services and testing for vulnerabilities. Physical firewall hardware is utilized to limit network/system access
Do you have a completed Shared Assessments full SIG questionnaire? Have you undergone a SAS 70 or SSAE 16 audit?	No.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

What internal controls do you currently have in place to audit the security configuration of any AWS or SaaS hosted applications – e.g., secure storage and database instances	Anti-virus software, HostMonitor software, Status screens (dedicated TVs with system status dashboard information for system administrators), Database transaction logs, IIS logs, Windows logs, Payment logs.
Risk Management practices - any other controls or process you can share?	All employees read and confirm understanding of PCI policies annually. These policies cover areas such as Confidential Data, Incident Response, External connections etc. In addition to understanding the established policies, employees are encouraged to identify potential risks or make suggestions, whether related to system administration, software development, QA testing, or support. When risks are identified appropriate personnel are notified and severity and priority are determined. Risks are logged and tracked in project management to be scoped and scheduled for resolution. Weekly team meetings and quarterly department assessments are made to discuss resolutions or status on outstanding resolutions.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

Data Center Information	
What are the requirements for the data center?	We use Rogers Data Centre in Ottawa, Ontario Canada. Physical servers are owned and operated by Tomahawk Technologies Inc. NOT Rogers. • PCI DSS, ISAE 3402 Type II, SSAE 16 SOC 1 Type II and CSAE 3416 Type II certifications • Unmarked facilities with single secure entrances for customers and staff • 100 percent CCTV security cameras (low-light technology) monitor facility interiors and exteriors 24x7 • Two-stage bio-metric authentication process (iris-scanners and encrypted access cards) • Individually locked cabinets that house servers Users with high level access permissions can add and remove who has access to the data center via contacting the company that runs the data center. A physical meeting is also required to get access for iris scans and card. A web portal lists users who have access to the data center with varying levels of permissions. Access is only granted to system administrators who require it to perform their duties (add new servers, hard drives, maintain existing, etc.) gain entry to the data center.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

What redundancy and availability does the data center provide?	• Fire Suppression • N+1 cooling redundancy, computer-controlled compressors, humidity control systems, hot aisle/cold aisle containment and perforated cabinet doors for enhanced temperature control. • Two-stage, pre-action dry pipe sprinkler system and/or gas suppression (extinguishes fire without water). • Network Redundancy • Backup generator • Rogers' private, nationwide Fiber Optic network includes over 25,000 km of fiber routes with connectivity to key network access points in the U.S. and overseas. Our multi-homed network is provisioned with extensive peering and Tier 1 transit providers. • Redundant Cooling System • 100% uptime • Sophisticated architecture design is guaranteed to protect your mission-critical applications and data against possible impact from single points of failure, with redundant connectivity, backup power and cooling.
Can the system be setup in multiple Data centers to support HA?	Yes, the system could be setup in multiple data centers to support a geographical separate HA installation. The same technologies that are used on the local system LAN could be replicated in a secure WAN environment.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141

SSO Implementation with OPS-COM	
Please describe how SSO is implemented in your solution.	SSO is implemented with standard client/server technology. Recent project implementation using CAS under Jasig. The Jasig open-source CAS server software integrates with several protocols for back-end SSO implementation. Whether local or remotely accessed, the CAS server offers a front line to SSO. • Supported SSO technology: SAML, LDAP, custom as scoped and developed for
Does your system require access to direct LDAP access for SSO in a hosted environment?	No, using a CAS server (as mentioned above) it would be possible to access LDAP without requiring direct LDAP access. In almost all cases this would be preferred implementation as this allows for future scalability without requiring any changes to the software. As an example, the Jasig CAS server supports proxy authentication using custom developed (or existing) plugin modules. Since the Jasig CAS project is a community driven project, it continues to mature and grow with added features.

92 Bridge Street • Carleton Place • ON • K7C 2V3
Toll Free: 855.410.4141 • Fax: 613.257.4141