Digital Monitoring Products, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to Meet the Trust Services Criteria for the Security Category for the Period of December 1, 2024, through November 30, 2025.

Table of Contents

Assertion of Digital Monitoring Products, Inc. Management 1
Assertion of Digital Monitoring Products, Inc. Management 2
Independent Service Auditor's Report 3
Independent Service Auditor's Report 4
Scope 4
Service Organization's Responsibilities 4
Service Auditor's Responsibilities 4
Inherent Limitations 5
Opinion 5
Digital Monitoring Products, Inc.'s Description of Its Commercial Security Products System 6
Section A: Digital Monitoring Products, Inc.'s Description of the Boundaries of Its Commercial Security Products System 7
Services Provided 7
Client Onboarding and Registration 7
Client Contracts 8
Client Deregistration 8
Client Support 8
Infrastructure 9
Software 9
People 10
Data 10
Processes and Procedures 11
Section B: Principal Service Commitments and System Requirements 12
Regulatory Commitments 12
Contractual Commitments 12
System Design 12

Assertion of Digital Monitoring Products, Inc. Management

Assertion of Digital Monitoring Products, Inc. Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Digital Monitoring Products, Inc.'s commercial security products system (system) throughout the period December 1, 2024, to November 30, 2025, to provide reasonable assurance that Digital Monitoring Products, Inc.'s service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in section A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2024, to November 30, 2025, to provide reasonable assurance that Digital Monitoring Products, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to commercial security products (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Digital Monitoring Products, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in section B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 1, 2024, to November 30, 2025, to provide reasonable assurance that Digital Monitoring Products, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Independent Service Auditor's Report

Independent Service Auditor's Report

David Roberts
Vice President of Cybersecurity
Digital Monitoring Products, Inc.
2500 Partnership Blvd.
Springfield, MO 65803

Scope

We have examined Digital Monitoring Products, Inc.'s accompanying assertion titled "Assertion of Digital Monitoring Products, Inc. Management" (assertion) that the controls within Digital Monitoring Products, Inc.'s commercial security products system (system) were effective throughout the period December 1, 2024, to November 30, 2025, to provide reasonable assurance that Digital Monitoring Products, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Digital Monitoring Products, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Digital Monitoring Products, Inc.'s service commitments and system requirements were achieved. Digital Monitoring Products, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Digital Monitoring Products, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements

- Assessing the risks that controls were not effective to achieve Digital Monitoring Products, Inc.'s service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Digital Monitoring Products, Inc.'s service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

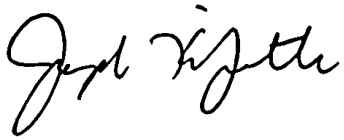
Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Digital Monitoring Products, Inc.'s commercial security products system were effective throughout the period December 1, 2024, to November 30, 2025, to provide reasonable assurance that Digital Monitoring Products, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

January 16, 2026



Digital Monitoring Products, Inc.’s Description of Its Commercial Security Products System

Section A: Digital Monitoring Products, Inc.'s Description of the Boundaries of Its Commercial Security Products System

Services Provided

Digital Monitoring Products (DMP) manufactures intrusion, fire, access control, and cellular alarm hardware, and designs corresponding software applications. In 2008, the organization launched SecureCom Wireless (SCW), a cellular data service provider that provides backend services for DMP products. SCW operates as part of DMP, and all SCW personnel report up to DMP personnel through the shared organizational chart. DMP is responsible for product development, while SCW is focused on the hosting of production servers and associated infrastructure, as well as providing operations and support for connectivity and backend services. DMP also works exclusively via a direct sales model, selling alarm systems to vendors who perform installation and management of DMP products.

Services provided by DMP are performed with the following three tools:

- Dealer Admin, which is the software as a service (SaaS) tool DMP's clients use to manage, update, and check status of DMP devices. Dealers can opt in to automatic firmware updates or choose to manually install updates. Bulk update tools are available through the platform.
- Virtual Keypad, which is the SaaS tool that consumers utilize to manage DMP devices, including adding and removing users, arming systems, and viewing video clips from integrated security cameras. Android and iOS applications are available for Virtual Keypad in addition to the web application.
- EASYconnect, which is a platform that provides Dealer Admin and Virtual Keypad connectivity to network and cellular-connected systems. EASYconnect features include TCP connections from security system hardware to EASYconnect servers, weather service to provide local weather indications, event service to send diagnostic information and user-selected events, and virtual private network (VPN) service for secure communication to cellular devices.

Client Onboarding and Registration

DMP primarily gains new clients via word-of-mouth, referrals from existing clients, and trade show attendance and support. The organization also utilizes in-person demonstrations and meetings with the Executive Team at corporate headquarters in Springfield, Missouri to market its products and services. Wintouch CRM is used to track client interactions and relationship progress. Information obtained and documented from clients during the onboarding process includes company name, address information, contact information, and licensing and order information.

Regional training managers participate in the client onboarding process by providing training that addresses DMP platforms and user responsibilities. Additionally, week-

long hardware bootcamps are held at the corporate headquarters to provide hardware training to clients.

Additionally, during registration dealer settings are input into Dealer Admin, including company names, addresses, zip codes, SCW license information, account numbers, and other tool configuration details. Two admin users are set up for the new dealer, and they follow an established process to create a password, update contact information, and modify basic settings.

Client Contracts

Standardized contracts are utilized with clients detailing terms and conditions of the business agreement, limitations of liability, warranties, and legal/regulatory considerations. Once a contract is in place with an installation vendor, Dealer Admin access is provisioned for the vendor via two admin accounts which can be utilized to update settings and contact information within the platform.

Client Deregistration

If a client declines to renew their contract, access to the admin portal is removed, but end users still have access to utilize Virtual Keypad.

Client Support

DMP provides ongoing support to its clients who, in turn, are responsible for providing support to their end users. However, DMP clients often contact DMP support on their client's behalf. DMP maintains in-house tech support and customer service teams, reachable by email or phone call. Calls are routed based on support type to relevant support personnel. Support supervisors monitor client support resolution timeliness, and an escalation process is in place to address issues that can't be handled via one email or phone call. Customer issues are tracked via Wintouch and Jira.

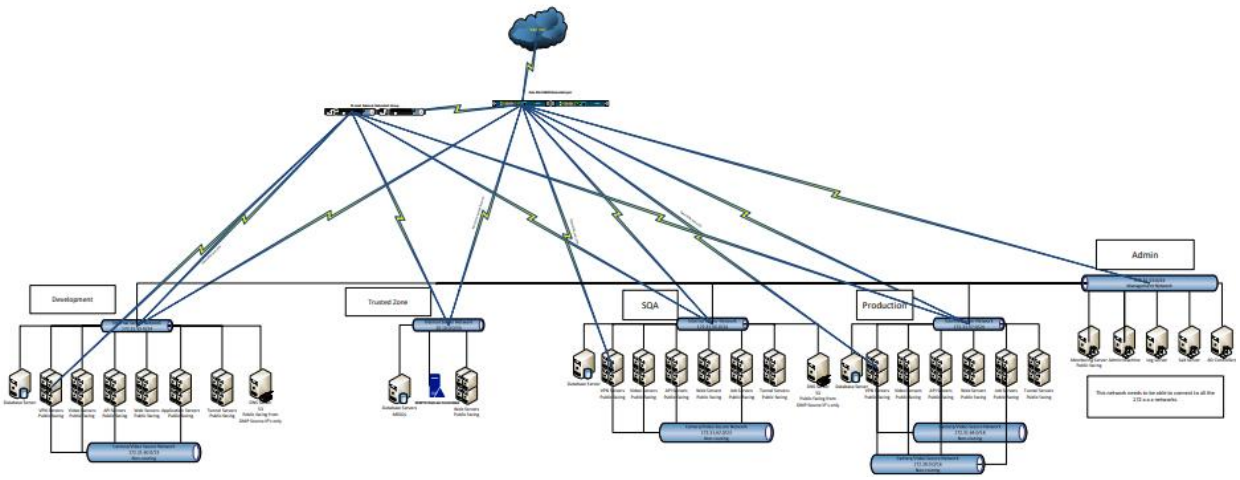
DMP's dealer clients can reach support via a dedicated phone line or via TechSupport@dmp.com, and in both cases, client requests are routed to appropriate support personnel based on type of support required and corresponding hardware type. Support contact information, including technical support, customer service numbers, and email addresses, are publicly posted.

Additionally, Dialpad is utilized to track metrics associated with incoming telephone-based support requests, including hold time, call disposition, call volume, average wait time, and customer satisfaction. Support supervisors perform weekly reviews of the tech support inbox to track email responses for each support personnel. These reviews are documented via reports detailing the number of unique emails and emails responded to per day for each relevant support personnel.

Escalated issues are tracked in Jira, and when relevant, bug tickets are linked to customer issues. Additional details tracked through Jira tickets include reporters (internal or external) and assignees. Dashboards in Jira are utilized to monitor time-to-resolution for client issues.

Infrastructure

DMP maintains a detailed network diagram of the LightEdge-hosted environment, including firewall connectivity, primary environments in place (which include the development environment, trust zone, staging, production, and admin environments), camera and video subnetworks, and VMware hosts. Separate diagrams are also maintained for each primary network, detailing specific assets in place in each network. The network diagram is included below:



Software

DMP uses the following software throughout its day-to-day operations:

- Google Chrome
- Linux
- Microsoft Visual C++
- Microsoft SQL Server
- Octopus Deploy Tentacle
- SentinelOne
- SolarWinds Client Component
- Ubuntu
- VMware Tools
- ManageEngine
- Rapid7

People

In the DMP 2025 Organizational Chart, it shows that the organization follows a traditional hierarchy, and the Executive Vice President of Corporate Strategy, Vice President of Production, Vice President of Cybersecurity, Vice President of International Sales, Vice President of Sales, Vice President of Industry Relations, Vice President of Training, Vice President of Product Management and Support, Chief Operating Officer, and Chief Financial Officer all report to the CEO and manage corresponding business teams and divisions. The Vice President (VP) of Cybersecurity is on the Security Council along with the Executive Director of Information Technology and the Director of SCW Infrastructure.

Data

The DMP Information Security Program addresses data security, including data classification and handling, information and asset labeling, logical access controls, encryption, security key and certificate management, and relevant physical access controls. The Executive Director of Information Technology and the Director of SCW Infrastructure are responsible for the protection of sensitive data.

The organization maintains detailed data flow diagrams that show the flow of data within Azure and LightEdge-hosted environments via HTTP/S, GraphQL, Remote Strings (proprietary), AMCP, RTSP, HLS, SMB, SFTP, OpenVPN, and SQL. Additionally, the Acceptable Use Policy addresses secure handling and permitted dissemination of information in accordance with classification level, classifying data as public, dealer, proprietary, confidential, or video.

For data encryption, DMP divides its encryption into three main areas: database encryption, application encryption, and operating system encryption. These are naturally subdivided by at-rest versus in-flight encryption. The organization's DBA, Manager of Infrastructure, and DevOps Sysadmin are involved with anything database encryption-related (specifically SQL encryption, etc.).

Encryption is performed for the SQL database. Data at rest is encrypted at the SAN level, including data within the LightEdge-hosted environments. Application encryption consists of Secure Sockets Layer (SSL)-protected web applications and API endpoints, with continuous evaluation in place to eliminate unencrypted streams and channels. BitLocker and similar OS-level encryption are used for OS-level encryption.

The Encryption Key and Certificate Management Policy governs the data classification of keys, access restrictions to keys, cryptoperiods and key rotation, key generation, key distribution and transportation, key backups, and roles and responsibilities related to key management. Keys and managed identifiers are utilized within AWS and Azure identity access management (IAM), and virtual machines (VMs) within Azure are encrypted at creation.

AES 256 keys are in place on SQL servers, and FIPS 140-2 level 1 validated encryption is in place on SCW Wireless SANs. The organization maintains a formal inventory of keys and certificates, tracking category, entry, issuer, and type for keys and certificates.

Additional details are tracked as relevant, including date of issue, status, and associated account.

DigiCert is utilized to generate SSL certificates, and API keys are generated via AWS, Google, or other associated sites. Keys are shared via the SCW Wireless' SecureShare application, which generates expiring URL links and AES 256-bit encryption. Key renewal tasks are scheduled and tracked via ManageEngine. The Executive Director of Information Technology and the Director of SCW Infrastructure are responsible for protection of data transmissions.

Changes are made with the approval of a supervisor (Manager of Infrastructure), and the processes vary depending on the type of encryption, steps required to implement the encryption, and the amount of potential downtime or maintenance required to configure. The organization continually evaluates the encryption of its applications and connection to critical systems to root out any possible unencrypted streams or channels. DMP has BitLocker and local Windows Firewall usage on the roadmap as well.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

Section B: Principal Service Commitments and System Requirements

Regulatory Commitments

DMP employs EDPO as its Data Protection Representative in the European Union (EU) and United Kingdom (UK). The organization is subject to General Data Protection Regulation (GDPR) requirements for its EU servers and utilizes data processing agreements within contracts for customers utilizing EU systems. The organization maintains and utilizes such agreements for GDPR compliance with customers utilizing EU-hosted systems. The organization also contracts with an independent CPA firm to perform annual assessments of the organization's consolidated financial statements.

Contractual Commitments

DMP maintains contracts and agreements with its employees, vendors, and clients. Employees are required to sign agreements addressing trade secrets, proprietary and confidential information, copyright, and non-solicitation, while client contracts follow a standard template and address the scope of service, terms and conditions, liability limitations, warranties, and regulatory considerations. Contractual documentation implemented with vendors addresses the non-disclosure of proprietary information for both parties, addresses scope of services, data processing, terms of the agreement, and DMP/SCW responsibilities.

System Design

DMP designs its commercial security products system to meet its regulatory and contractual commitments. These commitments are based on the services that DMP provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that DMP has established for its services. DMP establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in DMP's system policies and procedures, system design documentation, and contracts with clients.