SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON MANAGEMENT'S ASSERTION RELATED TO ITS

DW Cloud

Relevant to Security

For the period December 19, 2024 to March 19, 2025

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report

To the Management of Kaltec Enterprises Inc. (DW)

Scope

We have examined DW's accompanying assertion titled "Assertion of DW Management" (assertion) that the controls within DW's DW Cloud (system) were effective throughout the period December 19, 2024 to March 19, 2025, to provide reasonable assurance that DW'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 (With Revised Points of Focus — 2022)* in AICPA*, Trust Services Criteria.*

Service Organization's Responsibilities

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

Service Auditors' 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 AICPA. 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 DW'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 DW'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 DW's DW Cloud were effective throughout the period December 19, 2024 to March 19, 2025, to provide reasonable assurance that DW's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

San Jose, California

March 27, 2025

2. Assertion of DW Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Kaltec Enterprises Inc. (DW) DW Cloud (system) throughout the period December 19, 2024 to March 19, 2025, to provide reasonable assurance that DW's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of DW's DW Cloud," (description) 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 19, 2024 to March 19, 2025, to provide reasonable assurance that DW'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 (With Revised Points of Focus - 2022)* in AICPA*, Trust Services Criteria.*

DW'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 the accompanying system description.

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 19, 2024 to March 19, 2025, to provide reasonable assurance that DW's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by DW Management

March 27, 2025

3. Description of DW Cloud

Company Background

Kaltec Electronics, Inc. dba Digital Watchdog (‘Kaltec Electronics, Inc. dba Digital Watchdog’) was founded in 1987 with the objective of providing innovative security cameras, recorders, software and other hardware to the market.

Kaltec Electronics, Inc. dba Digital Watchdog has developed a solid reputation for product quality and performance, with the most reliable and feature-rich products and applications, protecting 60% of the Top 20 global brands, in Retail, Financial, Enterprise, Healthcare, Government and all other key vertical markets.

Services Provided

Kaltec Electronics, Inc. dba Digital Watchdog (‘Kaltec Electronics, Inc. dba Digital Watchdog’) provide innovative security cameras, recorders, software and other hardware to the market. Our ground-breaking DW Spectrum IPVMS (IP Video Management Software) includes a Software as-a-Service (SaaS) application known as DW Cloud.

DW Cloud is a multiuser SaaS application that allows end users to manage and access them digital recorders and security cameras from the Cloud and mobile apps.

The functions of DW Cloud include:

- Login with an email account.
- Access / Manage Digital/Network Video Recorders (DVR/NVR) systems.
- Access / View / Manage Digital Security Cameras.

Principal Service Commitments and System Requirements

As Kaltec Electronics, Inc. dba Digital Watchdog’s DW Cloud service is included with the DW’s Spectrum software, there are no Service Level Agreements (SLA) associated with the product.

Components of the System

Infrastructure

Primary infrastructure used to provide Kaltec Electronics, Inc. dba Digital Watchdog's Services system includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Network Optix	Sub-service provider	Network Optix develops, maintains, hosts and operates all functions of DW Cloud. They have provided DW with their SOC2 report.

Software

Primary software used to provide Kaltec Electronics, Inc. dba Digital Watchdog's Services system includes the following:

Primary Software	
Software	Purpose
Network Optix	Network Optix develops, maintains, hosts and operates all functions of DW Cloud. They have provided DW with their SOC2 report.

People

Kaltec Electronics, Inc. dba Digital Watchdog has staff organized in the following functional areas:

- Corporate. Executives, senior operations staff, and company administrative support staff, such as legal, compliance, accounting, finance, human resources, and product management. These individuals support DW Cloud at an overall corporate level.
- IT Support. IT supports internal users including corporate users, tech support, sales and marketing.
- Technical Support. The TS (Technical Support) department provides technical assistance to end users of DW Cloud.
- Operations/Development. Network Optix develops, maintains, and manages the DW Cloud service fully.

Data

The data collected by the system is the following:

- First Name
- Last Name
- Email
- Password

All information and security is handled by Kaltec Electronics, Inc. dba Digital Watchdog's third-party subservice provider Network Optix.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Kaltec Electronics, Inc. dba Digital Watchdog policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Kaltec Electronics, Inc. dba Digital Watchdog team member.

Logical Access and Physical Security

Access management processes exist so that Network Optix employee and contractor user accounts are added, modified, or disabled in a timely manner and are reviewed on a quarterly basis. In addition, password configuration settings for user authentication to DW Cloud are managed in compliance with Network Optix's Password Policy which is part of the Information Security policy.

Users must be approved for logical access by senior management prior to receiving access to DW Cloud. Management authorization is required before employment is offered and access is provided. Users must also be assigned a unique ID before being allowed access to system components. User IDs are authorized and implemented as part of the new hire onboarding process. Access rights and privileges are granted to user IDs based on the principle of least privilege and Role-Based Access Control (RBAC) protocols. Access is limited to that which is required for the performance of job duties for individual users, and generic access by Network Optix employees is not allowed.

AWS is responsible for restricting data center access to authorized personnel.

AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.

Computer Operations – Backups

For disaster recovery and restoration of services, Network Optix uses a combination of AWS S3 storage buckets and RDS (Relational Database Services) to store backups and database files and snapshots. For fault tolerance, backups are stored across multiple availability zones in encrypted vaults. Only personnel with administrative access can retrieve stored backups.

Computer Operations – Availability

An incident response policy and procedures manual has been formally documented and implemented to guide preparation, detection, response, analysis and repair, communication, follow-up, and training for any class of security breach or incident. The responsibilities in the event of a breach, the steps of a breach, and the importance of information security are defined for all employees. The Incident Response Team employs industry-standard diagnosis procedures (such as incident identification, registration and verification, as well as initial incident classification and prioritizing actions) to drive resolution during business-impacting events.

Network Optix reviews, triages, and communicates all incident alerts whereupon the Incident Response Team starts the incident response process. Post-mortems are convened after any significant operational issue, regardless of external impact. Documentation of the investigation is conducted to determine that the root cause is captured and that preventative actions may be taken in the future.

Change Control

A Change Management Policy has been formally documented and implemented to guide the processes of a change request, documentation, review, evaluation, approval, scheduling, testing and implementation. Changes that may affect system availability and system security are communicated to management and any partners who may be affected via email.

System configuration standards are formally documented and implemented to ensure that all systems and network devices are properly and securely configured. CIS and NIST hardening standards, as well as configurations in AWS, is used as a basis for Network Optix's system configuration standards.

Secure Software Development: Network Optix applies a systematic approach to software development so that changes to customer-impacting services are reviewed, tested, approved, and well-communicated. Prior to deployment to production environments, changes are:

- Developed: in a development environment that is segregated from the production environment. Customer content is not used in test and development environments.
- Reviewed: reviewed by peers for technical aspects and appropriateness.
- Tested: to confirm the changes will behave as expected when applied and not adversely impact performance.

Data Communications

The internal network is protected from public Internet traffic by using stateful inspection firewalls from Amazon's AWS. Network Optix utilizes AWS's security groups which are configured to deny traffic and only allow specific services to a specific destination. Access to administer the firewalls is restricted to only employees who have that responsibility. A security group acts as a firewall that controls the traffic allowed into a group of instances. For each security group, custom rules are added that administer the allowed inbound traffic to instances in the group

All other inbound traffic is denied. Encrypted communications are used to protect remote Internet sessions to DW Cloud and the internal network. Encryption is used to ensure the privacy and integrity of the data being communicated in transit over the public network.

Boundaries of the System

The boundaries of DW Cloud are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the DW Cloud.

The applicable trust services criteria and the related controls:

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- **Security**: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.

Control Environment

Integrity and Ethical Values

The effectiveness of controls is dependent on the integrity and ethical values of the people who implement, manage, and monitor them. Integrity and ethical values are important foundations of Kaltec Electronics, Inc. dba Digital Watchdog's control environment, affecting the design, implementation, and monitoring of the controls. Integrity and ethical behavior are supported by Kaltec Electronics, Inc. dba Digital Watchdog's culture, governance, hiring and onboarding practices, ethical and behavioral standards, the way those are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are

described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Kaltec Electronics, Inc. dba Digital Watchdog's competence of employees includes the knowledge and skills necessary to accomplish employees' roles and responsibilities, in support of Kaltec Electronics, Inc. dba Digital Watchdog's objectives and commitments. Management's commitment to competence includes careful consideration of the competence levels required for each role, the requisite skills, knowledge, and experience, and the performance of individuals, teams and the company.

Management's Philosophy and Operating Style

Kaltec Electronics, Inc. dba Digital Watchdog's management philosophy and operating style is a purpose-driven, risk-based approach to pursuing the company objectives and satisfying Kaltec Electronics, Inc. dba Digital Watchdog's commitments. Risk taking is an essential part of pursuing objectives. A formal approach is taken to understanding those risks and being deliberate about which risks are acceptable, and where risk mitigation actions are required.

Organizational Structure and Assignment of Authority and Responsibility

Kaltec Electronics, Inc. dba Digital Watchdog's organizational structure provides the framework within which its activities for achieving the objectives are planned, executed, managed, and monitored. An organizational structure has been developed to suit Kaltec Electronics, Inc. dba Digital Watchdog's needs and is revised over time as the company grows and requirements change.

Roles and responsibilities are further established and communicated through documented policies, and job descriptions, as part of individual performance review processes, reviewing and communicating team and functional performance, and the various operational team and governance meetings.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.

- Organizational charts are communicated to employees and updated as needed through groupware.

Human Resource Policies and Practices

Kaltec Electronics, Inc. dba Digital Watchdog's employees are the foundation for achieving the objectives and commitments. Kaltec Electronics, Inc. dba Digital Watchdog's hiring, onboarding and human resource practices are designed to attract, develop, and retain high-quality employees. That includes training and development, performance evaluations, compensation and promotions, providing personal support and perks for individuals, recognizing team and company success and building a culture of alignment to a shared purpose and vision. It also includes disciplinary processes and business planning to avoid single-person dependencies to ensure the objectives and commitments are not reliant on individuals.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

Kaltec Electronics, Inc. dba Digital Watchdog's risk assessment process identifies and manages risks that threaten the achievement of the objectives and commitments. This includes risks that may affect the security, reliability or integrity of the services provided to user organizations and other interested stakeholders.

A formal process is followed to identify, assess, treat, and monitor the risks to ensure the risks are aligned to the risk appetite and objectives of Kaltec Electronics, Inc. dba Digital Watchdog, and mitigated or avoided where appropriate. Risks identified in this process include:

- Operational risk – changes in the environment, staff, or management personnel, reliance on third parties, and threats to security, reliability, and integrity of Kaltec Electronics, Inc. dba Digital Watchdog's operations.
- Strategic risk – new technologies, changing business models, and shifts within the industry.
- Compliance – legal and regulatory obligations and changes.
- Financial – the sustainability of Kaltec Electronics, Inc. dba Digital Watchdog and resources supporting the objectives.

These risks are identified by Kaltec Electronics, Inc. dba Digital Watchdog management, employees, and third-party stakeholders, and updated in the risk register as a single source of monitoring the risks. The formal risk assessments ensure the ongoing commitment of

management, and support completeness and an evolving view of the risk landscape in Kaltec Electronics, Inc. dba Digital Watchdog's context.

Information and Communications Systems

Information and communication are a core part of Kaltec Electronics, Inc. dba Digital Watchdog's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control Kaltec Electronics, Inc. dba Digital Watchdog's operations effectively. The information and communication systems consider the internal control requirements, operating requirements, and the needs of interested parties including employees, customers, third-party vendors, and regulators.

The information and communication systems include central tracking systems that support Kaltec Electronics, Inc. dba Digital Watchdog's established processes, as well as various meetings, and documented policies, procedures and organizational knowledge.

Monitoring Controls

Management monitors the controls to ensure that they are operating as intended and that controls are modified and continually improved over time. Leadership, culture, and communication of the controls are important enablers to their effectiveness in practice. This ensures buy-in amongst the employees and empowers Kaltec Electronics, Inc. dba Digital Watchdog's team and individuals to prioritize the performance and continual improvement of the controls. Evaluations are performed during business, in management reviews, and by independent auditors to assess the design and operating effectiveness of the controls.

Deficiencies that are identified are communicated to responsible control owners to agree remediation actions or re-enforce the control requirements and importance. Corrective actions are tracked with agreed timelines and ownership for remediation with management, for ensuring appropriate actions are completed promptly.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to DW's DW Cloud.

Subservice Organizations

Kaltec Enterprises Inc.’s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to DW’s services to be solely achieved by DW ‘s control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of DW.

The following subservice organization controls should be implemented by Network Optix to provide additional assurance that the trust services criteria described within this report are met.

Security Category	
Criteria	*Controls expected to be in place*
CC4.1 - The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Network Optix is responsible for vulnerability scanning and the remediation of vulnerabilities identified.
CC5.2 - The entity also selects and develops general control activities over technology to support the achievement of objectives.	
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Network Optix is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	

Security Category	
Criteria	*Controls expected to be in place*
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Network Optix is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	Network Optix and AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Network Optix is responsible for incident monitoring and the remediation security incidents.
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.	

Security Category	
Criteria	*Controls expected to be in place*
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	Network Optix is responsible for incident monitoring and the remediation security incidents.
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Network Optix is responsible for authorization, design, development, configurations, documentation, testing, approving and implementation of changes to infrastructure, data, software of the entity's system.

DW management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, DW performs monitoring of the subservice organization controls, including the following procedures

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

Complementary User Entity Controls

DW's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to DW's services to be solely achieved by DW 's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of DW's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to DW.
2. User entities are responsible for notifying DW of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.

4. User entities are responsible for ensuring the supervision, management, and control of the use of DW services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize DW services.
6. User entities are responsible for providing DW with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying DW of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.