



Service Organization Control 3 (SOC 3[®])



DMS Technologies Inc.'s report on its
ebase Software relevant to Security &
Privacy for the period February 1, 2024
to May 31, 2024

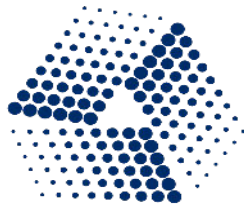




Table of Contents

Section I	1
DMS Technologies Inc.'s Management Assertion	2
Section II	3
Independent Service Auditor's Report	4
Attachment A	7
DMS Technologies Inc.'s Description of the Boundaries of its ebase Software	8
Infrastructure	9
Software	10
People	10
Policies, Processes & Procedures	10
Data	11
Attachment B	13
Principal Service Commitments and System Requirements	14



Section I
DMS Technologies Inc.'s Management Assertion



DMS Technologies Inc.'s Management Assertion

We are responsible for designing, implementing, operating and maintaining effective controls within DMS Technologies Inc.'s ("DMS Technologies") ebase Software ("system") throughout the period February 1, 2024 to May 31, 2024, to provide reasonable assurance that DMS Technologies Inc.'s service commitments and system requirements relevant to Security, Privacy were achieved. Our description of the boundaries of the system is presented in attachment 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 February 1, 2024 to May 31, 2024, to provide reasonable assurance that DMS Technologies Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Privacy ("applicable trust services criteria") set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Privacy, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). DMS Technologies 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 attachment 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 February 1, 2024 to May 31, 2024, to provide reasonable assurance that DMS Technologies Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by:

143A0710C2A34B5

Daryl Jones, VP of Technology and Engineering

DMS Technologies Inc.

June 26, 2024

Section II
Independent Service Auditor's Report



Independent Service Auditor's Report

To the Management of DMS Technologies Inc.:

Scope

We have examined DMS Technologies Inc.'s ("DMS Technologies") accompanying assertion titled "DMS Technologies Inc.'s Management Assertion" ("assertion") that the controls within the DMS Technologies Inc. ebase Software ("system") were effective throughout the period February 1, 2024 to May 31, 2024, to provide reasonable assurance that DMS Technologies Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Privacy ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Privacy, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service organization's responsibilities

DMS Technologies Inc. is responsible for its service commitments and system requirements and for designing, implementing and operating controls within the system to provide reasonable assurance that DMS Technologies's service commitments and system requirements were achieved. In Section I, DMS Technologies has provided the accompanying assertion titled "DMS Technologies Inc.'s Management Assertion" ("assertion"), about the effectiveness of controls within the system. When preparing its assertion, DMS Technologies 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 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 the Canadian Standard on Assurance Engagements 3000, Attestation Engagements Other Than Audits or Reviews of Historical Financial Information, set out in the *CPA Canada Handbook – Assurance* and with attestation standards established by the American Institute of Certified Public Accountants (AICPA). These 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 the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve DMS Technologies’s service commitments and system requirements based on the applicable trust criteria.
- Performing such other procedures as we considered necessary in the circumstances

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 achieve the service organization’s service commitments and system requirements based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design 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 the DMS Technologies Inc. ebase Software were effective throughout the period February 1, 2024 to May 31,



2024, to provide reasonable assurance that DMS Technologies's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated in all material respects.

Restricted use

Certain complementary subservice controls that are suitably designed and operating effectively are necessary, along with controls at DMS Technologies Inc., to achieve DMS Technologies Inc.'s service commitments and system requirements based on the applicable trust services criteria. Users of this report should have sufficient knowledge and understanding of complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements. DMS Technologies Inc. uses Microsoft Azure to provide cloud infrastructure services. Users of this report should obtain the relevant Microsoft Azure SOC2 or SOC3 report.

DocuSigned by:

MHM Professional Corporation

4F22774372B4BC...

Chartered Professional Accountant

Calgary, Alberta

June 26, 2024



Attachment A
DMS Technologies Inc.'s Description of the
Boundaries of its ebase Software



DMS Technologies Inc.'s Description of the Boundaries of its ebase Software

Company and Business Overview

Founded in 1995, DMS Technologies Inc. is located in St. Catharines, Ontario. We offer a wide range of products and services to the facilities management sector and are proud of our continued successes in providing effective and competitive solutions to industry challenges. Our experienced team of focused client service managers, software engineers and support staff have propelled DMS Technologies Inc. to one of the leading providers of FM software in Canada.

Today, our best-in-class, ebase Software provides Facility Managers across multiple sectors, throughout Canada with a premium digital tool to manage their organizations.

Services Provided

Our flagship software application, ebase provides clients with a robust, yet easy-to-use software suite that ensures facilities are managed efficiently and capital assets are used effectively. First launched in 2002, ebase is a hosted “software-as-a-service” (SaaS) model, providing access to users through a standard web-browser. Modules can be added to the system at any time and function independently of one another, although several can be integrated where standard client business policy and process apply. Each module is available through a subscription fee, providing unlimited users, support, maintenance, and training for one all-inclusive annual cost.

As a leader in the facilities management industry, ebase has assisted a diverse range of facilities management professionals over the past decade in improving workflow and facility management processes. We work closely with our clients, employing a user-driven approach to software to ensure that client solutions constantly evolve to reflect the unique needs of our users.

That user-driven approach has helped us create a solution that automates the core functions of facilities management into 18 customized modules that enhance processes to save money and time.



From simplifying the complexities of project management, to alleviating the frustration of routine tasks like log sheets, facility rentals, supply ordering, and program management, ebase's customized modules are designed to reflect the unique needs of your organization.

The Boundaries of the System Used to Provide the Services

The boundaries of the system are the specific aspects of DMS Technologies Inc.'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 supports the services provided to customers are not included within the boundaries of the system.

The components that directly support the services provided to customers are as described in the sections below.

Infrastructure

ebase is a SaaS-multi-tenant client-server application hosted on Microsoft Azure. All customers receive their own tenant of the ebase Software, and their data is logically separated and not accessible to other tenants to prevent unauthorized access.

The ebase application runs within Microsoft Azure using a geographically appropriate region (eg. Canada East or Canada Central for Canadian clients). The software is divided into an Application Server and a Database Server. The backend is written in PHP, and the frontend written in PHP, HTML, and JavaScript. Apache is utilized as the web server.

The database supporting the application utilizes Microsoft Azure running MySQL Server..



Software

The following provides a summary of software systems used to deliver DMS Technologies ebase Software:

- Microsoft Azure Monitor – used for the monitoring of production systems and log storage.
- Github – used for source code version control.
- Ubuntu Linux – operating systems to support operation of the system.
- PHP – programming language used to write the backend of the web application.
- Twilio SendGrid- used for sending application email

People

DMS Technologies has a defined organizational structure with specific roles, responsibilities, and appropriate lines of reporting required to support the ebase Software. It is comprised of, and supported by, the following teams who are responsible for the delivery and management of the system:

- Management – responsible for providing the overall direction, strategic vision, and management of DMS Technologies.
- Product – responsible for guiding the overall direction of the product roadmap including usability, enhancements, and new features.
- Engineering – responsible for front and back-end development of the in-scope applications and services. Also, responsible for oversight of software and data engineering, IT Infrastructure, and all IT related activities.
- Operations – responsible for day-to-day operations such as document processing and office functions.
- Sales – responsible for development of new business related to the DMS Technologies services.
- Customer Success - responsible for successful onboarding of customers on DMS Technologies platform and act as advocates for the continued success of the platform. They are responsible for product support issues, customer engagement and growth.

Policies, Processes & Procedures

Management has developed and communicated to employees and contractors a set of policies, processes, and procedures in several operational areas which support the



Security, Privacy objectives of the ebase Software. As part of the wider Information Security Management Program, DMS Technologies has developed and organized the following policies and procedure documents that are used to support the ebase Software.

The following policies and procedures are available to employees and contractors through the ebase Software:

- Acceptable Use
- Access Control
- Business Continuity and Disaster Recovery
- Change Management
- Corporate Ethics
- Customer Support and SLA
- Data Retention and Disposal
- Incident Management
- Information Security
- IT Asset Management
- Key Management and Cryptography
- Network Security
- Personnel Security
- Risk Assessment
- Server Security
- Software Development
- Vendor Management
- Vulnerability Management
- Workstation Security

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently to achieve policies and procedures compliance. DMS Technologies has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objective of the organization.

Data

DMS Technologies collects the following types of information through its ebase Software:



- Facility-related data applicable to the module(s) used within the ebase Software
- User supplied data and configurations applicable to the module(s) used within the ebase Software
- Activity and access logs

Data is entered via the client web application and sent to the application servers via RESTful API calls. The data is processed and written to the MySQL instance. Data transmission is secured using HTTPS/TLS 1.2 and does not leave the VPC. Data replication channels are also encrypted and transmitted via the private Microsoft Azure connection. All data access requests require an ACL context which contains both the authenticated user and the organization that is requesting the data. These requests are validated via the DMS Technologies permissions system to exclude the possibility of cross-client data leakage. All data at rest is encrypted using AES-256 encryption.

Attachment B
Principal Service Commitments and System
Requirements

Principal Service Commitments and System Requirements

DMS Technologies designs its processes and procedures related to its ebase Software to meet its objectives. Those objectives are based on the service commitments that DMS Technologies makes to user entities related to Security, Privacy, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that DMS Technologies has established for the services.

Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the ebase Software that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect customer data at rest and in transit.

Privacy commitments to user entities are documented in customer agreements. Privacy commitments are standardized and include, but are not limited to, the following:

- Maintaining a privacy officer and privacy policy accessible to clients.
- Restricting access to personal information for only necessary purposes.
- Responding to data requests and notification of data breaches in a timely manner.
- Establishing a process for disclosing personal information to third parties.
- Not selling client's and their customers' information and not sharing or disclosing data to third parties for purposes other than aligned to existing agreements.

DMS Technologies establishes operational requirements that support the achievement of Security, Privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in DMS Technologies system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the ebase Software.