DEVICIE

System and Organization Controls (SOC) for Service Organizations

SOC 3

For The

Devicie Solution

A Report on Devicie NA Inc. and Devicie PTY LTD's System and Controls Relevant to Security, Availability, and Confidentiality

May 1, 2025, to April 30, 2026

AssurancePoint
CPAs and Compliance Advisors

Report of Independent Service Auditors issued by AssurancePoint, LLC

TABLE OF CONTENTS

SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT 1

SECTION 2 MANAGEMENT'S ASSERTION 4

SECTION 3 DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM 6

OVERVIEW OF OPERATIONS 7
COMPONENTS OF THE SYSTEM 7
SUBSERVICE ORGANIZATIONS 12
COMPLEMENTARY USER ENTITY CONTROLS 12

SECTION 4 PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 14

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 15

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Devicie NA Inc. and Devicie PTY LTD:

Scope

We have examined Devicie NA Inc. and Devicie PTY LTD's ("Devicie") accompanying assertion included in Section 2 of this report that the controls within Devicie's Solution system were effective throughout the period May 1, 2025, to April 30, 2026, to provide reasonable assurance that Devicie's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Service Organization's Responsibilities

Devicie 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 Devicie's service commitments and system requirements were achieved. Devicie has provided the accompanying assertion, in Section 2, ("Management's Assertion") about the effectiveness of controls within the system. When preparing its assertion, Devicie 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 stated within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on 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.

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

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 Devicie'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 Devicie'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.

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 are 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 Devicie's Solution system were effective throughout the period May 1, 2025, to April 30, 2026, to provide reasonable assurance that Devicie's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Atlanta, Georgia
July 9, 2026

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within our Devicie Solution system throughout the period May 1, 2025, to April 30, 2026, to provide reasonable assurance that our service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Our description of the boundaries of the system is presented in Section 3 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 May 1, 2025, to April 30, 2026, to provide reasonable assurance that Devicie's service commitments and system requirements were achieved based on the applicable trust services criteria. Devicie'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 3.

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 May 1, 2025, to April 30, 2026, to provide reasonable assurance that Devicie's service commitments and system requirements were achieved based on the applicable trust services criteria.

SECTION 3

DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM

Overview of Operations

Company Background

Devicie provides automated device management software that helps organizations deploy, manage, and maintain Microsoft Intune environments at scale.

At Devicie, we help organizations improve security, productivity, and compliance through automated device management built on Microsoft Intune.

Description of Services Provided

Devicie helps organizations using Microsoft Intune achieve and maintain an optimal state of modern device management. The platform automates the build, deployment, and ongoing management of Intune configurations at scale.

With Devicie, organizations with Microsoft Intune achieve an optimal state of modern device management, increasing organizational productivity and strengthening their security posture, while freeing up IT and security resources.

The service provides automated processes for endpoint devices and application management via Microsoft Azure and Intune, including:

- Provisioning, packaging, and ongoing patching of devices, operating systems, and applications
- Monitoring for configuration drift and automatically remediating endpoints back to the ideal state
- Assured compliance with security frameworks
- Admin and custom configuration
- Standard Operating Environment (SOE) build and Autopilot
- Reporting on key endpoint health metrics

Devicie and customer data is held in the cloud utilizing Microsoft Azure services, including Azure Data Explorer (ADX), PowerBI, and Log Analytics. The data includes audit trails and monitoring data relevant to customer devices and activity. Security and performance reports are produced from this data.

Components of the System

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

The Devicie Solution and production infrastructure is hosted within the Microsoft Cloud Service (Azure). Devicie manages the protected information assets via an inventory that tracks, logs, and maintains asset records within the cloud console.

The in-scope infrastructure consists of multiple applications, systems, and databases as shown in the table below:

Primary Infrastructure	
Infrastructure Component	**Business Function Description**
Devicie Solution	End-user platform used to deploy, control, streamline, and maintain company-issued devices
Microsoft Azure	Cloud hosting service that hosts the Devicie Solution system's file storage, databases, applications, and containers
Microsoft Entra ID	Stores information about domain members, including users and applications, and allows administrators to manage permissions and control access to resources

Additionally, the following secondary systems and software are used to support the system:

Additional Software Supporting the System	
Software Component	**Business Function Description**
GRC Platform	Security and compliance application used to monitor Devicie's security and internal control posture and operational effectiveness
Microsoft 365	Contains the network directory, email, document, and calendar management
Microsoft Defender	Automated security assessment service analyzing the cloud production environment, resources, workloads, configurations, and applications for vulnerabilities, and security threats and issues
Security Information and Event Management (SIEM)	Cloud-native SIEM utilized to analyze volumes of data and to investigate and respond to malicious activities or anomalies within the cloud production environment
Vulnerability Scanning and Management	Third-party tool utilized to perform monthly security reviews and vulnerability assessments
Version Control System	Integrated Development Environment (IDE) and code repository utilized for hosting the Devicie Solution's source code and for software development version control, reporting, and project management
Microsoft Intune Mobile Device Management (MDM) System	MDM system utilized to centrally deploy, manage, and secure company-issued devices
Human resource information system (HRIS)	Used for payroll and people management
Customer Relationship Management & Finance Systems	Cloud-based CRM used for customer support, sales support, and financial management and reporting
Collaboration and Messaging	Internal messaging and collaboration tools
Ticketing and task management boards	Internal ticketing system used to manage and track projects and tasks

People

Personnel involved in the operation and use of the system are:

- Executive Management – Responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives
- Operations – Responsible for maintaining the availability and managing access and security of the cloud production environment. Members of the Operations team have access to the cloud production infrastructure. Members of the Operations team may also be members of the Engineering team.
- Product Development – Responsible for the development, testing, deployment, and ongoing maintenance and functionality of the system and managing the entire system lifecycle
- Information Technology and Support - Responsible for managing laptops, software, and other technology involved in employee productivity and business operations while emphasizing the utilization of security and efficiency of technology
- Engineering – Responsible for development of the orchestration and automation, and Devicie services, focusing on security and efficiency of technology. The Information Technology / Engineering teams also collaborate to manage data backups and recovery.

Data

User and account data collection is permitted under executed customer agreements (as well as other separate agreements with vendors, customers, suppliers, and other relevant third parties). Access to user and account data is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job functions.

The following table describes the information used and supported by the system:

Data Used and Supported by the System		
Data Description	**Data Usage**	**Classification**
Customer Data	Customer data is captured, utilized, managed, processed, and stored by Devicie in delivering its services.	Restricted

Procedures

Logical Access Infrastructure, Software, and Architecture

Devicie requires passwords to the cloud production infrastructure and version control software to be configured according to the company's Password Policy. When possible, Devicie integrates the production systems and services with the Entra ID Identity Management, using Security Assertion Markup Language (SAML), to control authentication and access privileges. A password manager tool is installed on employee workstations to maintain and secure personnel access credentials. The cloud production infrastructure and version control software can only be remotely accessed by authorized personnel possessing a valid multifactor authentication MFA method or security key. High security accounts with administrative rights to the cloud production infrastructure also require the use of hardware security keys. Devicie allocates access to information systems and services using role-based access control (RBAC) within the cloud production infrastructure to ensure that access is restricted based on job role and functions. Administrative access privileges to the cloud production infrastructure, version control software, and production application are restricted to authorized personnel. Further, Devicie restricts privileged access to the production databases to authorized personnel.

Access Authorization and Access Revocation

A formal Access Control Policy is in place to guide personnel in the requirements for adding, modifying, and removing existing access privileges. Devicie's onboarding process identifies appropriate roles and system access

for employees and contractors. Changes to information system access are processed through the internal ticketing system and approved by the hiring manager.

The leaver process includes disabling or removing access for terminated employees and contractors from information systems upon notification by the employee's or contractor's manager. Devicie conducts a manual access review at least annually to help ensure that access to information systems, applications, and resources is restricted to authorized personnel. Required changes are tracked to completion. Additionally, the security and compliance application performs continuous user account reconciliations on integrated Devicie systems to identify active user accounts within those systems and compare them to active personnel profiles within the security and compliance application and HRIS. Security personnel are notified upon any identified discrepancies.

Physical Security

Devicie personnel do not maintain physical access to the production infrastructure. This access is restricted to Microsoft Azure. See the Subservice Organizations section for further details on the controls expected to be implemented by Microsoft Azure.

Perimeter Security and Data Transmissions

Devicie does not manage the underlying infrastructure hosting the production application; therefore, limiting its responsibility for perimeter security to the application layer and logical access controls to its cloud production infrastructure. Devicie utilizes the cloud-native intrusion detection and prevention tool to provide continuous monitoring of the company's network and early detection of potential security breaches. Remote access to the cloud production infrastructure and version control software requires a valid MFA method or security token by authorized personnel. Devicie ensures the use of Transport Layer Security (TLS) encryption for the transmission of internal, confidential, or restricted information over public networks. Additionally, connections to the cloud production environment and APIs are secured using Hypertext Transfer Protocol Secure (HTTPS).

Devicie has an MDM system in place to centrally manage devices supporting the service. Employee workstations are configured with disk encryption.

Anti-malware

Employee workstations have enterprise endpoint security software installed to help protect Devicie's systems from malware, viruses, and other threats. Further, employee workstation operating system security patches are configured to be applied and enforced automatically. The unauthorized use or installation of software is explicitly prohibited in accordance with the company's Acceptable Use Policy.

System Monitoring

The monitoring of system components and detection of important events is necessary to achieve Devicie's security, availability, and confidentiality commitments and system requirements. Devicie has a formal Operations Security Processes document in place to help ensure that system configurations are deployed consistently throughout the cloud production environment. The security and compliance application is configured to monitor aspects of production and non-production systems through API connections in real time. The security and compliance application notifies users via email when expected configurations or manual procedures fall out of compliance with internal control requirements.

Production application baseline configurations are retained within the version control software and provides roll back capabilities anytime an approved baseline configuration change is made. Devicie utilizes the cloud-native security management and threat intelligence and protection tool to continuously monitor and detect threats and vulnerabilities within the cloud production infrastructure and resources. Devicie also utilizes the cloud-native SIEM tool to continuously ingest and analyze logs and metrics within the cloud production infrastructure and resources to detect, investigate, and respond to threats and anomalies. The tool is configured to alert appropriate personnel via a dedicated Slack channel upon detection of anomalies or unauthorized user account activity. Further, Devicie utilizes the cloud-native intrusion detection and prevention tool to provide continuous monitoring of the company's network and early detection of potential security breaches.

Devicie performs monthly security reviews and vulnerability assessments. The results and recommendations for remediation are reported during the quarterly Security Steering Committee meetings and are tracked within the internal ticketing system through resolution.

Incident Response

Devicie has a Security Incident Response Process in place that defines how personnel evaluate and respond to security failures, incidents, concerns, and other complaints. The Security Incident Response Process identifies the Security Team as the team responsible for responding to and managing any identified security events or incidents.

Security events are reported in a standard ticket that requires analysis, classification, and resolution of the event. If a security event is elevated to the classification of a security incident, the security incident is logged, tracked, and resolved within the internal ticketing system. Security incident documentation includes a description of the incident and any corrective actions taken to remediate the issue. Further, Devicie has formal business continuity and disaster recovery policies and procedures in place and performs disaster recovery testing annually. Production and customer data is continuously backed up to a geographically separate location and backups of API data connections are performed daily to help ensure data and systems can be recovered in the event of an incident.

Change Management

Devicie has a formal software development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology change requirements. Devicie requires changes to software and infrastructure components of the system to be reviewed and approved and pass the security vulnerability, dependency, and build pipeline testing prior to implementation to the cloud production environment.

Version control software is utilized to retain production application baseline configurations and provides roll back capabilities anytime an approved baseline configuration change is made. The version control software is configured to require additional approval for pull request prior to merging to the main branch. To help ensure the security of source code and to prevent unintentional changes to the cloud production environment, Devicie maintains logically segregated cloud development and cloud production environments. Devicie restricts access to implement changes to the cloud production environment to authorized personnel.

Capacity Management, Data Backup, and Disaster Recovery

Devicie incorporates a variety of processes to ensure the reliability and availability of its systems and services. Formally documented procedures are in place to guide personnel in availability, capacity, and performance monitoring of the cloud production infrastructure and information systems. Devicie utilizes the cloud-native observability and logging tools to continuously monitor the availability, performance, and capacity of the cloud production infrastructure. The tools are configured to send email notifications in the event of an exceeded metric or threshold.

The Operations Security Processes formally document the requirements for the backup and recovery of production and customer data. To safeguard against data loss, Devicie utilizes an automated backup tool to continuously backup production and customer data to a geographically separate location. The cloud-native automated backup tool is also configured to perform daily backups of the production application API data connections. A multi-location strategy is deployed within the cloud production environment to permit the resumption of operations in the event of a loss of a cloud data center facility. Business continuity and disaster recovery policies and procedures are in place. Devicie performs annual testing of the disaster recovery process and procedures.

Identification and Maintenance of Confidential Information

Devicie has established a Data Security and Classification Policy in place to guide personnel in the secure retention and disposal of company and customer data. Confidential or sensitive customer data is prohibited from being used or stored in non-production systems and environments according to the Data Security and Classification Policy. A defined data classification scheme is in place within the Data Security and Classification Policy for the labelling and handling of data and enforces controls and procedures based on the classification that includes safe handling, storage, retention, and destruction of data. TLS encryption protocols are in place to encrypt internal, confidential, and restricted data in transit

To uphold confidentiality and employee and contractor accountability, employees and contractors formally acknowledge a confidentiality agreement or confidentiality statements during onboarding.

Disposal of Confidential Information

To safeguard customer information, Devicie purges and wipes customer data containing confidential information from employee workstations prior to reuse or release. Additionally, Devicie purges or removes customer data containing confidential information from the cloud production infrastructure upon customer termination of service.

Subservice Organizations

The cloud hosting services provided by Microsoft Azure were not included within the scope of this examination.

The following table presents the applicable trust services criteria that are intended to be met by controls at Microsoft Azure, alone or in combination with controls at Devicie, and the types of controls expected to be implemented at Microsoft Azure to achieve Devicie's service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by Azure	Applicable Trust Services Criteria
Microsoft Azure is responsible for managing the encryption of production and customer data at rest.	CC6.1, CC6.7, C1.1
Microsoft Azure is responsible for ensuring access to their respective facilities and the physical information assets hosted within their respective facilities is restricted to authorized personnel.	CC6.4
Microsoft Azure is responsible for ensuring physical media containing production and customer data is securely sanitized or destroyed prior to being removed from their respective data centers or protected areas within their data hosting facilities.	CC6.5
Microsoft Azure is responsible for ensuring environmental protection controls are in place within the data centers housing the underlying production infrastructure.	A1.2

Complementary User Entity Controls

Devicie'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 of the applicable trust criteria related to Devicie's services to be solely achieved by Devicie's control procedures. Accordingly, user entities, in conjunction with the Devicie Solution system and related services, should establish their own internal controls or procedures to complement those of Devicie.

The following complementary user entities controls should be implemented by user entities to provide additional assurance that the applicable trust 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.

#	Complementary User Entity Control	Related Applicable Trust Criteria
1.	User entities are responsible for restricting and periodically reviewing privileged and administrative access within their Microsoft Entra ID and Intune environments, including the assignment of Global Administrator and other elevated access roles.	CC6.1
2.	User entities are responsible for safeguarding credentials used by their personnel to access Devicie Solution system and their own Intune tenants environments, including implementing and maintaining multifactor authentication where appropriate.	CC6.1

#	Complementary User Entity Control	Related Applicable Trust Criteria
3.	User entities are responsible for assigning users to the appropriate groups within the Devicie Solution system and periodically reviewing group memberships to ensure users are granted only the access necessary to perform their job responsibilities.	CC6.2, CC6.3
4.	User entities are responsible for defining and approving the users, groups, and devices to which Devicie Solution system configurations and policies are applied.	CC6.2, CC6.3
5.	User entities are responsible for notifying Devicie in a timely manner of personnel terminations, transfers, role changes, or other events that may require modification or removal of access.	CC6.2, CC6.3
6.	User entities are responsible for reviewing reports, alerts, and notifications provided by Devicie and taking appropriate action on items requiring user entity review or response.	CC7.1, CC7.2, CC7.3, CC7.4

SECTION 4

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Devicie designs its processes and procedures related to the Devicie Solution system to meet its objectives. Those objectives are based on the service commitments that Devicie makes to user entities, the laws and regulations that govern the Devicie Solution system, and the financial, operational, and compliance requirements that Devicie has established for the services.

Security, availability, and confidentiality commitments are documented and communicated to user entities in executed customer agreements. The principal service commitments are those commitments that apply to the broad base of users. Principal service commitments are standardized and include the following:

Security

- Devicie will restrict access to production and customer data.
- Devicie will monitor, detect, and remediate occurrences of unauthorized access.
- Devicie will identify, analyze, and remediate security events, security incidents, vulnerabilities, and breaches.
- Devicie will implement measures to protect the security of system data in transit and at rest.
- Devicie will hold employees to integrity and ethical standards during employment and hold employees accountable for their internal control responsibilities in the pursuit of objectives.
- Devicie will perform a risk assessment at least annually to identify and remediate risks to security and internal control objectives, the Devicie Solution, and supporting systems to an acceptable level.
- Devicie will communicate control deficiencies to the parties responsible for taking corrective action.
- Devicie will ensure that changes are formally authorized, documented, tested, and approved prior to implementation into the cloud production environment.

Availability

- Devicie's key services operate on a 24x7 basis, with continuous automated monitoring and active support during business hours.
- Data stores housing production, application program interface (API), and confidential data will be backed up according to the defined backup requirements.
- Devicie will maintain and test the disaster recovery process annually to minimize the impact of any potential business disruptions.

Confidentiality

- Customer data is not disclosed to unauthorized parties without written consent.
- Customer data is deleted from employee workstations during the employee termination process.
- Customer data is deleted from the application environment and supporting systems when customers leave the service.

System requirements are those requirements implemented to achieve Devicie's service commitments. System requirements are communicated in Devicie's 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 internal business systems and networks are managed, and how employees are hired, trained, and managed.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.