Panopto®

SOC 3

REPORT ON MANAGEMENT'S ASSERTION ON THE EFFECTIVENESS OF CONTROLS
WITHIN THE VIDEO CONTENT MANAGEMENT SYSTEM
RELEVANT TO SECURITY AND AVAILABILITY
FOR THE PERIOD MAY 1, 2023 TO APRIL 30, 2024

AND INDEPENDENT SERVICE AUDITOR'S REPORT THEREON

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations™

TABLE OF CONTENTS

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

SECTION I: INDEPENDENT SERVICE AUDITOR'S REPORT

Panopto, Inc.
Pittsburgh, Pennsylvania

SCOPE

We have examined Panopto, Inc.'s (Panopto) accompanying assertion titled "Management Assertion of Panopto, Inc." that the controls within Panopto's Video Content Management System (system) were effective throughout the period May 1, 2023 to April 30, 2024 to provide reasonable assurance that Panopto's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 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

Panopto 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 Panopto's service commitments and system requirements were achieved. Panopto has also provided the accompanying assertion about the effectiveness of controls. When preparing its assertion, Panopto 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 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.

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

Our examination included the following:

- 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 Panopto's service commitments and system requirements based on the applicable trust services criteria.

Schneider Downs & Co., Inc.
www.schneiderdowns.com
PrimeGlobal
An Association of Independent Accounting Firms

One PPG Place
Suite 1700
Pittsburgh, PA 15222
TEL 412.261.3644
FAX 412.261.4876

65 E. State Street
Suite 2000
Columbus, OH 43215
TEL 614.621.4060
FAX 614.621.4062

1660 International Drive
Suite 600
McLean, VA 21102
TEL 571.380.9003

- performing procedures to obtain evidence about whether controls within the system were effective to achieve Panopto'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 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 Panopto's Video Content Management System were effective throughout the period May 1, 2023 to April 30, 2024, to provide reasonable assurance that Panopto's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schneider Downs & Co., Inc.

Pittsburgh, Pennsylvania
June 11, 2024

SECTION II: MANAGEMENT ASSERTION OF PANOPTO, INC.

We are responsible for designing, implementing, operating, and maintaining effective controls within Panopto, Inc.'s (Panopto) Video Content Management System throughout the period May 1, 2023 to April 30, 2024 to provide reasonable assurance that Panopto's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Point of Focus—2022)* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system (description) is presented in Section III 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, 2023 to April 30, 2024, to provide reasonable assurance that Panopto's service commitments and system requirements were achieved based on the applicable trust services criteria. Panopto'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 III.

Panopto uses a subservice organization to provide cloud infrastructure hosting. In addition, Panopto's services were designed with the assumption that certain controls would be implemented by user entities. The description in Section III presents the complementary controls that Panopto assumes have been implemented, suitably designed, and operating effectively at the subservice organization and user entities. The description does not disclose the actual controls at the subservice organization and user entities. Certain trust services criteria can be met only if the complementary subservice organization and user entity controls assumed in the design of Panopto's controls are suitably designed and operating effectively, along with the related controls at Panopto. We monitor the effectiveness of controls at the subservice organization on an annual basis.

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, 2023 to April 30, 2024, to provide reasonable assurance that Panopto's service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:

09AF0CE9156E4ED...

Brandon Nastoupil, SVP of Operations

June 11, 2024

Date

SECTION III: DESCRIPTION OF PANOPTO, INC.'S VIDEO CONTENT MANAGEMENT SYSTEM

SYSTEM OVERVIEW

Introduction

This document describes the control structure of Panopto, Inc. (Panopto or Company) as it relates to its hosted Video Content Management System (VCMS), a comprehensive platform to create, manage, share, search, and view video. As this description is intended to focus on features that are relevant to internal control for Panopto customers and other specified parties, it does not encompass all aspects of the services provided or procedures followed by the Company.

Panopto helps businesses and universities create secure, searchable video libraries of their institutional knowledge. Since 2007, the Company has been a pioneer in video capture software, video content management systems, and inside-video search technology. Today, Panopto's video platform is the largest repository of expert learning videos in the world. Headquartered in Pittsburgh, with staff located in London, Hong Kong, Singapore, and Sydney, Panopto has received industry recognition for its innovation, rapid growth, and company culture.

Background and Overview

Panopto's service offering is a cloud-based video platform for creating and delivering professional quality video:

- Creation and curation: Recording and streaming video presentations, online training, product demonstrations, lectures, and meetings using the Panopto desktop application or mobile app. Customers also may upload video captured elsewhere.
- Management and sharing: Hosting video content in a secure cloud-based central repository. The VCMS integrates with major single sign-on solutions for access control and governance.
- Video playback: Playback of single or multi-camera videos, interactive notes, content, and discussion via an HTML5 player. Videos can be embedded in any web page with complete support for viewing on mobile devices.
- Search and discovery: Support for automatic speech recognition (ASR) and optical character recognition (OCR) for inside-video search.
- Integration: Panopto offers built-in integrations for popular learning management systems (LMS), content management systems (CMS), customer relationship management systems (CRM), and enterprise portals.
- WAN and internet video sharing: Hypertext Transfer Protocol (HTTP)-based streaming across corporate wide area networks (WANs) and the internet.
- Implementation and customer support: Panopto provides full implementation and multiple customer support plan options.

Panopto may offer licensees certain third-party services in connection with the licensed products, such as video captioning.

Subservice Organizations Excluded from the Scope of the Examination

Panopto utilizes Amazon Web Services (AWS) to host its cloud computing infrastructure.

Boundaries of the System

The boundaries of the system encompass the services and controls described throughout this report.

Infrastructure

The VCMS enables customers to use Panopto software hosted on Panopto servers. Panopto's Cloud is hosted on Amazon Web Services (AWS) with geographic hosting options in the United States, European Union, Canada, Singapore, and Australia.

Panopto Cloud is secure and scalable, has high availability for redundancy, and is built to ensure uptime and reliability. Panopto software is installed on Amazon Elastic Compute Cloud (EC2) instances, using Amazon Simple Storage Service (S3) for content storage and Amazon CloudFront as the content delivery network.

Software

The following table details the key software components that support the VCMS:

Component	Description
Web servers	Microsoft Windows Server /Internet Information Services (IIS)
Application servers	Microsoft Windows Server Microsoft PowerPoint Amazon Simple Queue Service AWS Linux 2/Microsoft .NET core/Ffmpeg/Gstreamer
Database servers	Microsoft Windows Server /Microsoft SQL Server
Network	Active Directory
Search database	AWS Linux 2/Solr Cloud
Agile project management	Jira
Change management	GitHub Enterprise
Security event incident monitoring	Logz.io
Vulnerability scanning	MegaPlanIT
Customer support ticketing	Salesforce
Endpoint antimalware protection	Panda Adaptive Defense 360
Patch management	Automox
Workflow automation	Fresh Service
Identity and access management	OneLogin
Governance, risk, and compliance	Onspring GRC Suite

People

Panopto has a staff of approximately 170 employees and contractors organized in the following functional teams:

Team	Responsibilities
Corporate/General & Administrative	Senior executive management Back-office operations (administrative support, legal, contracting, accounting, finance, human resources)
Account Management and Customer Success	Software renewals Upselling and cross selling Account planning and forecasting Market research and competitive analysis Client relationship management
Business Development	Strategic partnerships Channel partnerships/OEM integrations
Customer Support	Technical support Customer feedback
Information Security Risk and Compliance	TX-RAMP program Security risk assessment Third-party risk management Security awareness and training Incident response
Operations	Sales operations/renewal operations CRM and marketing operations
Professional Services	Training and Onboarding Content Migration
Development and Engineering	Application development Server operations
Information Technology	Desktop hardware and software Troubleshooting and user support Network security Network and business application account management

Processes and Procedures

Panopto's Information Security Risk and Compliance Program (Program) is designed to safeguard information assets against unauthorized access, disclosure, modification, or loss. Panopto has developed, documented, and communicated procedures underlying key workflows that serve as the basis for controls.

Data

Panopto classifies all customer content and data as confidential. The Company does not use or share the information collected on behalf of a customer except when explicit permission from the customer is granted for support purposes, to contract with the customer, or as set forth in the Terms of Use and Privacy policy. The following types of data are created, collected, processed, and stored by the VCMS:

- Customer-generated content.

- Error reports and usage analytics.
- User profile information; and
- Production logs.

Third-Party Access

Panopto utilizes third-party captioning services for those customers who elect to purchase captioning. The service providers have access only to content explicitly sent to them for captioning and have the ability to report back billing information or error information in addition to captioning information to the VCMS.

Principal Service Commitments and System Requirements

The relationship between Panopto and its customers is expressed in the terms of contracts, agreements, and order forms. Service commitments and system requirements, along with restrictions, reporting obligations, service information, pricing and support services are set forth in the executed documents.

The Company's principal service commitments are to:

- Maintain commercially reasonable physical, electronic, and procedural safeguards that are designed to protect customer confidential information from unauthorized disclosure, modification, or destruction.
- Maintain the privacy of customer personal data as outlined in the Panopto Privacy Policy.
- Comply with applicable laws and regulations, including information security and data protection laws.
- Maintain availability of access to the hosted solution based on stated service-level objectives in the applicable Software License and Services Agreement.
- Provide support services according to the time frames established in the applicable Software License and Services Agreement.
- Notify customers promptly if the Company becomes aware of any incident affecting the confidentiality or security of customer information.

Panopto establishes operational and system requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other applicable requirements. These requirements include the implementation of logical access controls, user access reviews, risk and vulnerability management, personnel controls, system monitoring, incident response, and change management. Such requirements are communicated in Panopto's policies and procedures, system design documentation, and agreements with customers.

Information security policies define an organization-wide approach to how systems and data are protected. 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 VCMS.

USE OF SUBSERVICE ORGANIZATION AND COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

When selecting third-party vendors and service providers, Panopto evaluates the anticipated role of the organization to determine the risk to both customer data and the achievement of Panopto's service commitments. Panopto evaluates the service provider's ability to maintain appropriate security and privacy measures to protect confidential information. Third-party service provider contracts include requirements for implementing and maintaining appropriate security and privacy controls.

Each user entity's internal controls must be evaluated in conjunction with Panopto's controls and the related complementary subservice organization controls expected to be implemented at the subservice organization.

Panopto utilizes AWS to host its cloud computing infrastructure. Panopto expects that certain controls will be implemented by AWS to meet the applicable trust services criteria, either alone or in combination with the controls at Panopto, as described below:

<table>
<tr><th colspan="2">Security Category</th></tr>
<tr><td>Criteria</td><td>Controls expected to be in place</td></tr>
<tr><td>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.</td><td rowspan="4">AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Panopto's systems reside.</td></tr>
<tr><td>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.</td></tr>
<tr><td>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.</td></tr>
<tr><td>CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</td></tr>
<tr><td>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.</td><td>AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Panopto's systems reside.</td></tr>
</table>

Security Category	
Criteria	*Controls expected to be in place*
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. 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.	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components, including firewalls, routers, and servers where Panopto's systems reside.

Availability Category	
Criteria	*Controls expected to be in place*
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	AWS has appropriate environmental controls in place to protect data centers housing Panopto's servers and backups.

COMPLEMENTARY USER-ENTITY CONTROLS

In designing its VCMS, Panopto assumed that user entities would implement certain controls that, in combination with Panopto controls, are necessary to provide reasonable assurance that Panopto's service commitments and system requirements are achieved. It is each interested party's responsibility to evaluate the user entity control considerations presented in this section in relation to the internal controls that are in place at customer organizations in order to obtain a complete understanding of the total internal control structure and assess risk surrounding the Panopto VCMS.

Organizational and Administrative

1. User entities are responsible for providing the appropriate training to end-users on proper use of the Panopto Service consistent with the Terms of Service at https://www.panopto.com/terms-of-service/.
2. User entities are responsible for establishing documented policies and procedures for the transfer and sharing of information via the Panopto Service within their organization and with third parties.
3. User entities are responsible for identifying and managing the inventory of information assets on the Panopto Service.
4. User entities are responsible for obtaining necessary permissions and consents relating to their provision of content.

Logical Access

1. User entities are responsible for implementing additional password control configurations outside of the standard Panopto settings. (CC6.1)
2. User entities are expected to implement adequate controls over the granting and termination of user access to reasonably ensure that new users are properly authorized and terminated users are properly disabled. (CC6.2, CC6.3, CC6.4, CC6.5)
3. User entities are expected to perform periodic assessments of their end-users' permissions to reasonably ensure that the access of their users is properly authorized. (CC6.2)
4. User entities are responsible for ensuring the secure disposal of confidential customer data consistent with their data retention policies. (CC5.3, CC6.5)
5. User entities are expected to configure the inactivity timeout setting to automatically log users out after a predefined inactivity interval and require users to reauthenticate with their username and password. (CC6.6)

Incident Management

1. User entities should train end-users on their responsibilities and organizational procedures for identifying, handling, and responding to security incidents pertaining to the use of the Panopto Service.
2. User entities should contact Panopto if there are any issues with service availability or security, including, but not limited to, unauthorized use of their password or account, compromise of data, or security events

www.schneiderdowns.com