Report on Contentful Inc.’s Contentful Subscription Services Relevant to Security, Availability, and Confidentiality Throughout the Period January 1, 2025 to May 31, 2025

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Contentful Inc. ("Contentful")

Scope

We have examined Contentful's accompanying assertion titled "Assertion of Contentful Inc. Management" (assertion) that the controls within the Contentful Subscription Services (system) were effective throughout the period January 1, 2025 to May 31, 2025, to provide reasonable assurance that Contentful'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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

Contentful uses subservice organizations to provide Platform-as-a-Service (PaaS) and 24/7 security threat detection and response services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Contentful, to achieve Contentful's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Contentful's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Contentful 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 Contentful's service commitments and system requirements were achieved. Contentful has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Contentful 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 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 Contentful'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 Contentful'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 the Contentful Subscription Services were effective throughout the period January 1, 2025 to May 31, 2025, to provide reasonable assurance that Contentful's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Contentful's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
July 4, 2025

Section 2

Assertion of Contentful Inc. Management

Assertion of Contentful Inc. ("Contentful") Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Contentful Subscription Services (system) throughout the period January 1, 2025 to May 31, 2025, to provide reasonable assurance that Contentful'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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, Trust Services Criteria. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

Contentful uses subservice organizations for Platform-as-a-Service (PaaS) and 24/7 security threat detection and response services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Contentful, to achieve Contentful's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Contentful's controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2025 to May 31, 2025, to provide reasonable assurance that Contentful's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Contentful's controls operated effectively throughout that period. Contentful'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 January 1, 2025 to May 31, 2025, to provide reasonable assurance that Contentful's service commitments and system requirements were achieved based on the applicable trust services criteria.

Contentful Inc.

Attachment A

Contentful Inc.’s Description of the Boundaries of Its Contentful Subscription Services

Type of Services Provided

Contentful Global, Inc. (“Contentful” or “the Company”) and its affiliates offer a Software as a Service (SaaS) cloud-based content management and publication platform. This service enables registered users to upload, manage, and publish content using Contentful Application Programming Interfaces (APIs) and graphical user interfaces.

Contentful has global operations with primary office hubs located in Berlin, Germany; and Denver, CO, United States (US); with secondary office locations in London, United Kingdom; New York, NY, US; and San Francisco, CA, US.

Contentful affiliates include:

- Contentful Inc., United States
- Contentful (Germany) LLC, United States
- Contentful GmbH, Germany
- Contentful (UK) Limited, United Kingdom
- Contentful (Ireland) Limited, Ireland
- Contentful (Netherlands) B.V, Netherlands
- Contentful (Denmark) ApS, Denmark

The Contentful Subscription Services (Contentful Services) comprise the following components:

- Contentful Platform: Headless Content Management System (CMS)
- Contentful Studio: Visual Experience Builder that requires Contentful Platform
- Content Delivery API (CDA): Read-only API for delivering content to applications and platforms
- GraphQL Content API: Read-only GraphQL API for accessing Contentful content
- Content Management API (CMA): Read/write API for content creation, updates, and deletion
- Content Preview API (CPA): Read-only API to preview content before publishing
- Images API: Read-only API for retrieving and manipulating images at delivery
- Web App: Web administration interface to configure platform settings and define content models

Excluded from the system description are the following:

- Ninetailed GmbH (Germany)
- Contentful Ecosystem: Marketplace Apps: Integrations and plugins for Contentful Services
- Contentful Ecosystem: Third-party Integrations: Third-party integrations and apps not owned or provided by Contentful
- Contentful Personalization (formerly known as Ninetailed by Contentful): Artificial Intelligence (AI)-native personalization platform

The boundaries of the system in this section details the Contentful Subscription Services. Any other Company services are not within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of Contentful Services 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 Contentful Services.

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

Infrastructure

The Company utilizes Amazon Web Services (AWS) to provide the resources to host Contentful Services. The Company leverages the experience and resources of AWS to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Contentful Services architecture within AWS to ensure the availability, security, and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure		
Business Function	**Operating System**	**Hosted Location**
Content Delivery Network (CDN)	Managed Service	AWS Global
Fully managed NoSQL database service	Managed Service	AWS US/EU Regions
Managed Kubernetes service	Managed Service	AWS US/EU Regions
Cloud compute service to support Amazon EKS	Amazon Linux	AWS US/EU Regions
Managed relational database service	Managed Service	AWS US/EU Regions
Scalable object storage service	Managed Service	AWS US/EU Regions
Cloud services and infrastructure	Managed Service	US, Ireland, Germany
Encryption key lifecycle management	Managed Service	AWS US/EU Regions
Serverless compute service	Managed Service	AWS US/EU Regions
Isolated virtual networks	Managed Service	AWS Global

Software

Software consists of the programs and software that support Contentful Services (operating systems [OSs], middleware, and utilities).

Third-party software — commercial and open-source software (OSS):

- All third-party software used for Contentful business or installed on Contentful equipment must be pre-approved by Security and Information Services and be appropriately licensed.

The list of software and ancillary software used to build, support, secure, maintain, and monitor Contentful Services include the following services, as shown in the bullets below:

- Cloud-based continuous delivery tool for Kubernetes to automate, manage, and secure the deployment of applications to Kubernetes clusters by using Git repositories as the single source of truth for application configurations.
- CDN and cybersecurity platform that enhances web performance, reliability, and security. It optimizes the distribution of customer content by routing traffic through its global network, reducing latency and improving load times.
- Cloud-based media management platform and CDN optimized for images and videos. Its CDN capabilities ensure fast delivery of media assets to users worldwide.
- Managed Detection and Response (MDR) provider that delivers security services to proactively monitor, detect, and respond to security threats on a 24/7 basis.
- CDN that specializes in real-time content delivery and edge computing. It allows for rapid distribution of dynamic and static content by caching it closer to the end user.
- Cloud-based platform for version control and collaboration, designed to facilitate the management of software development projects. It enables teams to collaborate on code, track changes, and manage project workflows, enhancing productivity and ensuring the integrity and security of the codebase.
- Cloud-based identity management platform that provides identity and access management solutions. It manages and controls access to applications and systems efficiently, ensuring secure authentication, authorization, and user management.
- Platform to aggregate and correlate logs for the purpose of monitoring and response.
- Cloud-based platform that facilitates Infrastructure-as-Code deployment automation, enabling the organization to provision, manage, and scale its infrastructure efficiently and securely.
- Platform to manage Human Resources (HR) information for all employees and contractors.
- Customer service and support platform designed to improve customer interactions and streamline support processes. It helps to manage customer queries, issues, and feedback.

People

The Company develops, manages, and secures Contentful Services via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Leadership Team (ELT)	The ELT function at Contentful provides management direction for the Security Program, with direct ELT sponsorship provided by the Contentful Chief Technical Officer (CTO). The ELT is responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.

People	
Group/Role Name	**Function**
Engineering	The Engineering function at Contentful develops, tests, deploys, and maintains the software that powers Contentful Services. Key responsibilities include managing the full software development lifecycle, overseeing cloud-based infrastructure to ensure scalability and performance, and integrating security practices to address vulnerabilities. The team also drives innovation through research and continuous improvement, collaborating with other departments to align engineering efforts with business goals and compliance requirements.
Product	The Product function at Contentful manages the product lifecycle from concept to launch, ensuring alignment with customer needs and organizational goals. Key responsibilities include overseeing product development to meet strategic objectives, designing secure and user-friendly experiences, and driving innovation through market research and data insights. The team also supports compliance with industry standards and regulatory requirements and embeds business resilience into products to ensure continuity during disruptions.
Customer Experience	Customer Experience incorporates services to support the customer experience including Customer Success, Learning and Professional Services. The Customer Experience function at Contentful handles customer inquiries and resolves issues in line with support plans. The team serves as the first point of contact, managing access to customer data securely while processing requests. The team provides technical and account-related assistance to meet SLAs and escalate critical issues to Engineering for prompt resolution, ensuring data protection throughout.
Security	The Security function at Contentful is responsible for leading the Company's cybersecurity program. This includes incident prevention and response, overseeing the implementation of information security policies, identifying and addressing vulnerabilities throughout the organization, and leading business resiliency efforts. The team facilitates the identification, assessment, and mitigation of organizational risks, ensures compliance with regulatory requirements, and promotes a culture of security across the organization.
People	The People function at Contentful oversees the entire employee lifecycle, ensuring effective and compliant management from recruitment to offboarding. Key responsibilities include managing recruitment and onboarding to attract and integrate top talent, overseeing performance and talent development, and administering compensation and benefits. The team ensures secure handling of HR data, compliance with legal standards, and efficient workplace operations.
Legal	The Legal function at Contentful ensures compliance with legal obligations and effectively manages legal risks to protect the organization. Key responsibilities include providing expert legal counsel on issues such as adherence to applicable laws and regulations, risk assessments, and formal investigations, while supporting incident management with strategic advice and evidence handling. The team oversees communications to ensure regulatory compliance and safeguard the Company's reputation, manages contracts and corporate governance, and ensures regulatory compliance.

People	
Group/Role Name	**Function**
Finance	The Finance function at Contentful ensures the organization's financial health and compliance, supporting growth and sustainability through effective oversight and decision-making. Key responsibilities include managing budgeting, forecasting, and financial analysis to align performance with business objectives; overseeing accounting, reporting, and tax compliance; and ensuring accurate revenue recognition. The team also handles Information Services, procurement, payroll, cash management, and investment strategies to maintain financial security.
Information Services	The Information Services function leads all internal information technology (IT) efforts at Contentful, focusing on managing workstations and access control systems and on ensuring efficient use of business applications. Key responsibilities include maintaining workstation security standards, overseeing robust access control measures, and performing secure onboarding and offboarding processes. The team also manages internal business applications to support efficient and secure operations across the organization.
Business Operations	The Business Operations function at Contentful drives strategic initiatives and enhances organizational efficiency by aligning operational strategies with company goals and market demands. Key responsibilities include developing and executing strategic plans, creating competitive pricing and packaging models based on market analysis, and optimizing business processes for improved effectiveness.

The following organization chart reflects the Company's internal structure related to the groups discussed above:

Figure 1: Contentful Global, Inc. Organization Chart

Procedures

Procedures include the automated and manual procedures involved in the operation of Contentful Services. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, and people operations. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of Contentful Services:

Procedures	
Procedure	**Description**
Logical and Physical Access	Describes the controls in place to safeguard access to Contentful systems and services, including the AWS-hosted infrastructure's physical security and Contentful's logical access measures, such as Single Sign-On (SSO) with Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and quarterly access reviews.
System Operations	Describes Contentful's processes for secure system operations, including monitoring and incident response with Endpoint Detection and Response (EDR) technology, Web Application Firewalls (WAFs), security groups, network segmentation, data backup and recovery, vulnerability management, and secure software development practices.
Change Management	Describes the process for planning, authorizing, implementing, and reviewing changes to Contentful's systems, processes, and infrastructure to maintain confidentiality and availability.
Risk Mitigation	Describes Contentful's framework for identifying, assessing, and mitigating information security risks, guided by a defined Risk Appetite and supported by a centralized Risk Register, annual risk assessments, and documented treatment plans to address risks based on their likelihood and impact.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the API, the customer defines and controls the data they load into and store in the Contentful Services production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, transmitted, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for the transmission of confidential or sensitive information over public networks. Encryption is enabled for data stores housing sensitive customer data.

The following table details the types of data contained in the production application for Contentful Services:

Data	
Production Application	**Description**
Contentful Platform Contentful Studio	**User Activity Data:** The Company keeps track of user activity in relation to the types of services customers and their users use, the configuration of their services, and performance metrics related to their use of the services, which can be used to address performance problems and flaws in applications. Log files are immutable records of computer events about an OS, application, or user activity, which form an audit trail.
Contentful Platform Contentful Studio	**User Profile Data:** The Company receives information about customers and their users, including name, email, and username. These records may be used to assist in authenticating and authorizing users and to investigate and mitigate security violations.

Data	
Production Application	**Description**
Contentful Platform Contentful Studio	**Customer Content:** Data submitted to and managed by customers in Contentful Services that the Company processes on behalf of its customers.

User Entity Responsibilities

Management of user entities is responsible for the following, which should not be regarded as a comprehensive list of all controls that should be employed by user entities:

- User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames.
- Controls to provide reasonable assurance that the Company is notified of changes in:
  - User entity vendor security requirements.
  - The authorized users list.
- It is the responsibility of the user entity to have policies and procedures to:
  - Inform their employees and users that their information or data is being used and stored by the Company.
  - Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
- User entities grant access to the Company's system to authorized and trained personnel.
- It is the responsibility of the user entity to implement controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
- User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.
- User entities deploy backup responsibilities outlined in the Security Addendum (Standards).

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS and a Managed Security Service Provider (MSSP) as subservice organizations for Platform-as-a-Service (PaaS) and 24/7 security threat detection and response services, respectively. The Company's controls related to Contentful Services cover only a portion of the overall internal control for each user entity of Contentful Services.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at AWS and the MSSP related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS' environmental protection controls should mitigate the risk of fires, power loss, climate, and

temperature variabilities. CSOCs are expected to be in place at the MSSP related to security threat management controls. The MSSP's security threat management controls should mitigate the risk of undetected or untimely responses to security threats impacting the system.

Company management receives and reviews the AWS and the MSSP SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by AWS and the MSSP to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS and the MSSP management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to Contentful Services to be achieved solely by the Company. The CSOCs that are expected to be implemented at the subservice organizations are described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	• AWS encrypts databases in its control.
CC6.4	• AWS restricts data center access to authorized personnel. • AWS monitors data centers 24/7 by closed circuit cameras and security personnel.
CC6.5 CC6.7	• AWS securely decommissions and physically destroys production assets in its control.
CC6.6	• AWS patches infrastructure supporting the service as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
CC7.2 A1.2	• AWS installs fire suppression and detection and environmental monitoring systems at the data centers. • AWS protects data centers against a disruption in power supply to the processing environment by an Uninterruptible Power Supply (UPS). • AWS oversees the regular maintenance of environmental protections at data centers.
CC7.3 CC7.4 CC7.5	• The MSSP identifies, logs, and evaluates security events and incidents. • The MSSP communicates escalated security events to Contentful personnel.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Contentful designs its processes and procedures for delivering Contentful Services to align with its objectives. These objectives are guided by the service commitments made to user entities; the applicable laws and regulations governing service provision; and the established financial, operational, and compliance standards.

Commitments are declarations made by management to customers regarding the performance of Contentful Services. These commitments are communicated through written contracts and, where applicable, customized customer agreements. Standardized agreements include:

- Subject to customer tier, a Terms of Service (ToS) or Master Subscription and Services Agreement (MSSA)
- Data Processing Addendum (DPA)
- Service Level Agreement (SLA)
- Security Addendum (Standards)

System requirements outline how Contentful Services must operate to fulfill the Company's commitments to user entities and are detailed in the Company's policies and procedures and Security Addendum.

The Company’s principal service commitments and system requirements related to Contentful Services include, but are not limited to, the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Contentful will maintain a security program that sets forth the administrative, technical, and physical safeguards to preserve the security, availability, and confidentiality of Contentful Services. • In the event Contentful becomes aware of a security breach resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to customer content, Contentful will notify affected customers without undue delay.	• Security Program • Security Policies • Security Incident Response • Data Breach Notification • Risk Management • Secure Development and Change Management • Personnel Security • Vulnerability Management • Network and System Security • Storage and Transmission Security
Availability	• Contentful will maintain the applicable service component availability set forth in the SLA. • Scheduled maintenance will not exceed four hours per calendar month, and Contentful will make commercially reasonable efforts to schedule maintenance during off-peak hours to minimize disruptions and avoid impacting the availability of the system.	• API Availability • Disaster Recovery Plan and Tests • Backups • Business Resilience and Continuity

Trust Services Category	Service Commitments	System Requirements
Confidentiality	• Contentful will delete (such that it cannot be recovered or reconstructed) customer content within its possession or control within 35 days of a written request by the customer upon termination or expiration of the agreement. • Confidential information is used solely per the customer agreement. Any required disclosure by law will include written notification, and breaches of confidentiality will be promptly communicated in writing.	• Secure Disposal, Deletion, and Storage of Customer Content • Confidential Information and Data Classification