VitalSource®

# Content Security: A Guide for Evaluating Best Practices

get.vitalsource.com

# VitalSource Content Security

## What you need to know about Content Security

The demand for digital learning materials and online modalities is growing. Publishers are increasingly distributing their content through a variety of technologies, platforms, and channels. This rapid digital expansion can jeopardize content integrity and security. Publishers' intellectual property, revenue, and reputation may be at risk, whether from bad actors seeking to steal and commercialize stolen content, or unauthorized sharing and usage of material.

**Your content is your business. Protecting it is ours.**

We provide the highest level of protection for our customers—it is paramount to our mutual success. Our commitment extends beyond our platforms; our goal is to educate our partners on the critical security measures needed to protect content, regardless of where that content lives.

# How do you know you are in good hands?

Asking these questions will help you understand and evaluate security measures during every critical step of the content storage and distribution process, so you can be assured that your content is properly protected.

1. How is content protected during delivery?
2. How is content kept/stored securely?
3. What digital rights management and piracy countermeasures are in place while distributing and licensing content?
4. What monitoring and alert systems are in place, and how are customers informed of an intrusion?
5. How and how often are external validations performed?

# Delivering Content

ASK: How is content protected during delivery?

**RISK: During the transfer process, your content may become lost or vulnerable.**

**EXPECT**

1. A well-explained workflow for content delivery
2. A delivery mechanism which is secure, including a secure transport (i.e., sftp, or https for web interface)
3. If being done manually, a unique set of credentials for each user that delivers content
4. If an integrated delivery, a secure API with unique credentials
5. Delivery systems that are routinely scanned and audited for vulnerabilities

**EXEMPLARY**

Audits for all of the above by an external firm

# Content Storage

ASK: How is content kept/stored securely?

**RISK: Content that is not properly protected while stored can be vulnerable to breaches.**

**EXPECT**

1. All content stored securely at rest and during transition using at least AES256 encryption
2. Access to content restricted to a limited number of people internally with this list of people audited routinely
3. Content that is no longer needed for distribution routinely and safely purged

**EXEMPLARY**

Secure logging and audit of internal access to content

# Digital Rights Management

ASK: What digital rights management (DRM) and piracy countermeasures are in place while distributing and licensing content?

**RISK: Without proper DRM, content protection and content access may not meet the publisher's requirements, resulting in loss of revenue and putting intellectual property at risk.**

**EXPECT**

1. Encryption during the movement of content between any two devices or platforms

2. Data encrypted or secured in motion and at rest

3. Only encrypted content distributed externally and read only while the application is in use

4. Each asset encrypted with a unique key

5. Online access restricted to one concurrent login

# Digital Rights Management

6. Downloads restricted to preset number of devices per active license

7. DRM and licensing models inspected and audited regularly

8. Countermeasures against scripts and scraping applications

9. Countermeasures against rooted devices and debuggers

10. Applications that use compile time obfuscation and key hardening

**EXEMPLARY**

Encryption keys that are unique to each user's device

# Monitoring & Alerts

ASK: What monitoring and alert systems are in place, and how are customers informed of an intrusion?

**RISK: As new threats emerge; they need to be identified and addressed to minimize exposure.**

**EXPECT**

1. Active monitoring and alerting for intrusion and piracy attempts
2. Monitoring of well-known internet locations where content piracy is discussed
3. Properly set user and system thresholds that alert on improper activity

**EXEMPLARY**

Staff that is on call and responds to security alerts and issues 24/7

# External Validation

Ask: How and how often are external validations performed?

**RISK: The vendor has gaps in the implementation of their security and anti-piracy programs.**

**EXPECT**

1. Platforms hosted in data centers certified as ISO 27001 and PCI/DSS
2. Third-party systems and services undergo thorough third-party technical and contractual due diligence
3. Ongoing intrusion and penetration testing
4. Third-party audits on a regular basis

**EXEMPLARY**

SOC II Certification

## The VitalSource Advantage
## Compliance, Standards, and Affiliations Checklist

Do your learning and digital content management platforms and tools meet and exceed industry standards in privacy, security, and accessibility?

Use the VitalSource Advantage Compliance, Standards, and Affiliations Checklist to ensure that you are investing in the most secure and compliant technologies available.

*Current as of April 2020

| PRIVACY | VitalSource |
|---|---|
| Zero PII integration options for maximum user privacy | ✓ |
| Family Educational Rights and Privacy Act (FERPA) Conformance | ✓ |
| Children's Online Privacy Protection Act (COPPA) Conformance | ✓ |
| General Data Protection Regulation (GDPR) Conformance | ✓ |
| California Consumer Privacy Laws Conformance | ✓ |
| UK Data Protection Act of 2018 Conformance | ✓ |
| Safe Harbor Privacy Shield Conformance | ✓ |

| ACCESSIBILITY | VitalSource |
|---|---|
| DAISY Consortium Friend | ✓ |
| WCAG 2.1 AA accessibility conformance documentation | ✓ |
| Long time sponsor of the NFB | ✓ |
| Winner of the 2019 Accessibility in Publishing DAISY award | ✓ |
| ASPIRE Gold rating | ✓ |
| Helped create the EPUB accessibility specification | ✓ |
| Content Transparency Initiative | ✓ |
| Accessibility metadata feed to our partners | ✓ |

| EDTECH INTEGRATION | VitalSource |
|---|---|
| IMS Member & LTI Certification | ✓ |
| LTI-Advantage Certification | ✓ |
| LTI Deep Linking & Grade Return | ✓ |
| COUNTER compliant | ✓ |
| CALIPER Certification | ✓ |

| SECURITY | VitalSource |
|---|---|
| Payment Card Industry Data Security Standard (PCI-DSS) Support | ✓ |
| 2 factor authentication for administrative access | ✓ |
| RSA public/private key | ✓ |
| CloudFlare | ✓ |
| Cloud Armor | ✓ |
| DRM hardening technologies | ✓ |

| LEARNER TOOLS | VitalSource |
|---|---|
| Offline App support for IOS, Android, Mac & Windows PLUS Kindle Fire and Chromebook | ✓ |
| Localized in U.S English & 36 other languages | ✓ |
| **INTEGRATED STUDY TOOLS** | **VitalSource** |
| Search in book and entire library | ✓ |
| Fast highlights mode | ✓ |
| Text read aloud | ✓ |
| Figure search | ✓ |
| Citations | ✓ |
| Visual display adjustment | ✓ |
| Review Mode | ✓ |
| Export to Microsoft OneNote | ✓ |
| Flashcard creation | ✓ |
| Assignment Creation | ✓ |

| TRUST AND SCALE | VitalSource |
|---|---|
| SOC II report covering security, privacy and confidentiality available<br>AICPA SOC 2 | ✓ |
| 24x7x365 access to Tier 1 support in English and Spanish with support facilities in North America | ✓ |
| Disaster Recovery protocols and geographically separated sites live and maintained | ✓ |
| Infrastructure hosted on Premium tier of GCP. North America served from U.S. based data center | ✓ |
| Over 120 global end points for content access | ✓ |
| Proven robust platform servicing millions of users and billions of requests each month worldwide | ✓ |
| World class content security trusted by thousands of publishers | ✓ |
| Best-in-class platform uptime | ✓ |

**At VitalSource, we are proud of the decades long commitment to protecting our customers' content and helping them expand their digital footprint, safely.**

Our security measures are best-in-class and continuously evolve to provide protection throughout the entire content distribution workflow. These protections are tested and validated externally, and we only use third-party technologies that do the same.

These are the standards that all technology companies should meet to be fully and operationally committed to content security.

# Keep your intellectual property safe without limiting your reach.

**To learn more about VitalSource's commitment to content security, visit get.vitalsource.com/resources/insights.**