Guide to Data and Security in BriefCatch

December 2023

Table of Contents

Introduction

We deeply value the trust that our customers place in us, and the protection of their personal and sensitive data stands paramount in our endeavors. Recognizing the importance of stringent data protection, we have instituted rigorous privacy, security protocols, and policies to safeguard the information entrusted to us. Our commitment to security and privacy is unwavering and is reflective in every facet of our operations. Furthermore, we believe in maintaining complete transparency with our customers regarding the treatment of their information.

This document brings together key technical, compatibility, security, privacy, and data protection information from various sources within the BriefCatch environment, including our SOC-2 report.

Company Information

Contact Details

LawCatch, Inc.
PO Box 593
Falls Church, VA 22040
+1.601.265.3778
https://briefcatch.com
help@briefcatch.com

Directors

Ross Guberman, Chief Executive Officer

Overview

BriefCatch is a legal writing software company that was founded in 2017 by legal writing expert Ross Guberman. The company's mission is to help lawyers improve their writing skills by using natural language processing to identify issues and provide real-time feedback. BriefCatch is based in Arlington, Virginia and serves the legal industry, specifically attorneys and law firms, by providing enterprise tools to enhance the quality of their written work.

Software Information

BriefCatch 3 is a software system powered by natural language processing that is designed to help legal professionals improve their writing skills and create more persuasive and effective documents. The system works by analyzing written documents and providing users with real-time feedback on elements

such as sentence length, readability, and word choice. The software analyzes documents for tone, readability, and grammar.

Technical Requirements by Product

We currently offer two versions of the BriefCatch legal writing product: BriefCatch 3 and BriefCatch Standalone. BriefCatch 3 is the current version of our flagship legal writing platform and is where all future development will be focused. BriefCatch Standalone is offered to organizations who do not meet the technical requirements for BriefCatch 3.

BriefCatch 3

BriefCatch 3 is a cloud-based product leveraging the latest Microsoft Azure Centralized Deployment capabilities and offers simple installation on user workstations via a Microsoft Office Add-In. All new features and functionality are developed for and deployed to the current, cloud-based product, so we recommend it to all subscribers who meet Microsoft's technical requirements (below).

Technical Requirements for BriefCatch 3

- Microsoft Word: Version 1704 or later of Microsoft 365 Business licenses.
    - On a Mac, Version 15.34 or later.
- Exchange Online
    - On Premises Exchange environments are not compatible with Microsoft Azure Centralized Deployment.

BriefCatch Standalone

For customers who do not yet meet the technical requirements to leverage BriefCatch 3, we offer BriefCatch Standalone, which is a COM/VSTO add-in. Deployed to user workstations via EXE or MSI file, all data processing for BriefCatch Standalone is conducted on the local user workstation.

Technical Requirements for BriefCatch Standalone

- Windows PC.
- Microsoft Word 2013 or later.

Subservice Organizations

BriefCatch 3 uses cloud services provided by the following providers: Google Cloud Platform, Amazon Web Services, and Microsoft Azure. These cloud services are used to host and manage various aspects of the BriefCatch 3 platform, including storage, processing, communication, and security.

Certifications

BriefCatch is SOC-2 Type 1 Compliant

BriefCatch is SOC-2 Type 1 compliant, having achieved our certification in 2023 with the support of an independent audit by Strike Graph, which confirmed BriefCatch's controls related to its information security practices, policies, procedures and operations met the rigorous SOC 2 standards for Security as developed by the American Institute of Certified Public Accountants (AICPA).

By adhering to the rigorous requirements of SOC-2 Type 1, we assure our clients that their data is handled with the utmost care and subject to stringent security protocols. Our SOC-2 Type 1 compliance underscores our ongoing efforts to maintain the highest standards of security and our dedication to providing our clients with the peace of mind they deserve when entrusting us with their valuable information.

Our Cloud Service Providers Maintain an Extensive List of Certifications

We have partnered with the world's foremost cloud service providers to deliver BriefCatch: Microsoft Azure, Google Cloud Platform, and Amazon Web Services. These organizations are renowned for their high availability and unmatched security measures, consistently upholding the pinnacle of security and compliance standards.

Google Cloud Platform

The Google Cloud Platform regularly undergoes independent verification of security, privacy, and compliance controls, achieving certifications against global standards. The Google Cloud Platform has earned and maintains an extensive list of certifications necessary to deliver some of the world's most demanding and sensitive enterprise applications, including:

- CSA STAR Level 2: Attestation
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27110
- ISO 27701
- SOC 1
- SOC 2
- SOC

Microsoft Azure

Azure compliance offerings are based on various types of assurances, including formal certifications, attestations, validations, authorizations, and assessments produced by independent third-party auditing firms, as well as contractual amendments, self-assessments, and customer guidance documents produced by Microsoft. Current compliance offerings include, but are not limited to:

- CSA STAR Levels 1-3
- ISO 20000
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701
- SOC 1
- SOC 2
- SOC 3

Amazon Web Services

Amazon Web Services' compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance. Current compliance offerings include, but are not limited to:

- CSA STAR Level 2: Attestation
- ISO 27001
- ISO 27017
- ISO 27018
- SOC 1
- SOC 2
- SOC 3

Data Privacy

At LawCatch, we are committed to ensuring that our customers have clarity and control over their data and can make informed choices regarding its use.

Application Data

We do not collect, log, or retain the text from your documents. No one can use, view, or reconstruct any of your document text at any point in processing.

Data Location

All BriefCatch data centers and servers are geo-located within the United States. Data transfers are managed strictly in accordance with applicable regulatory requirements.

Privacy Policy

At LawCatch, Inc., we are deeply committed to protecting your privacy and ensuring the security of your personal information. We collect various data including your personal details, information about your usage of the BriefCatch Platform, device specifics, and more, which are crucial for delivering and enhancing our services. Our use of your data ranges from providing services, improving user experience, to ensuring legal compliance and operational efficiency. All this data is securely stored in United States-based data centers. We also uphold your data protection rights, offering you control over your personal information with options for access, correction, deletion, and more, in accordance with applicable laws. For a comprehensive understanding of our data handling practices, we encourage you to read our full Privacy Policy here https://briefcatch.com/privacy-policy. This detailed policy provides an in-depth view of our dedication to data protection and your privacy rights.

Retention and Removal

You retain complete control over your data. We comply with all applicable regulatory requirements to enable users to request the deletion of their personal data from our systems. Data retention and destruction policies are maintained to comply with industry best practices. Read more about these practices and how users can exercise their rights at https://briefcatch.com/privacy-policy/.

Usage Data

We may collect data about how our users interact with the BriefCatch product for two purposes:

- Reporting purposes, for Enterprise administrators interested in understanding how frequently their users are accessing the product.
- Product improvement purposes, ensuring that our offerings evolve based on real user interactions and needs.

Usage data may be aggregated and anonymized in some circumstances and may be associated with the user's name and email address in others (e.g., Enterprise reporting).

Security and Data Protection

Safeguarding the integrity of our customer information and systems stands paramount in our operational commitments. Recognizing the critical nature of this responsibility, we have meticulously designed and implemented a comprehensive suite of technical security controls.

Access Control

BriefCatch incorporates the use of a Logical Access Policy that aims to prevent unauthorized access under the control of the organization by establishing and maintaining access rights management procedures.

Physical Access

All BriefCatch employees work from remote locations with employees using encrypted communications, antivirus, and locally encrypted hard drives to ensure data security measures are implemented.

BriefCatch does not own any physical locations or property where customer data or sensitive information may be stored. All of BriefCatch's risk sensitive business is conducted in the cloud, with access carefully secured via IAM policies in Google Cloud Platform, Amazon Web Services, and Microsoft Azure and role-based access in applications as necessary. BriefCatch relies on the physical access controls provided by Google Cloud Platform, Amazon Web Services, and Microsoft Azure to ensure servers, hard drives, and networking equipment are carefully secured in data centers.

Logical Access

To gain access to sensitive resources such as the BriefCatch 3 development environment, code repository or databases, a ticket must be requested, reviewed, and approved prior to any modifications to user access being made. Access to a particular resource that is no longer required should be terminated upon regular review, with a ticket documenting the process. This helps ensure the security and confidentiality of data under the control of the organization and reduces the risk of unauthorized access.

The classification of assets such as hardware, software, and data within the organization are based on their level of sensitivity or importance to apply appropriate access rights to the assets and ensure that only authorized personnel have access to them. Employees are responsible for safeguarding and managing the appropriate use of information using secure channels where appropriate as outlined in BriefCatch's Data Classification Policy.

The Password Policy sets password settings and controls that apply to all systems, ensuring that passwords are complex and changed regularly. MFA is enabled on all cloud-computing platforms (Google Cloud Platform, Amazon Web Services, Microsoft Azure), critical services, and applications when requested by management. Passwords must enforce a minimum

complexity of lowercase letters, uppercase letters, numbers, and special characters. Access is reviewed by the Compliance Team at least annually.

Third Party Access

No third-party providers have direct access to BriefCatch 3 data as BriefCatch 3 is only processed in Google Cloud Platform, Amazon Web Services, and Microsoft Azure data centers where strict policies and procedures are enforced to protect customer data and prevent unauthorized access.

Change Management

BriefCatch has a Change Management Policy which governs deliberate changes to IT production environments. The policy outlines a standardized change process to ensure technology acquisition, development, deployment, and maintenance processes are governed by change management procedures that may include one or more of the following activities:

- Planning and assessing the change
- Communicating the change to relevant stakeholders
- Testing the change
- Authorizing and deploying the change
- Documenting the change
- Reviewing the change for future improvements

Application-specific changes should be developed based on secure coding guidelines and industry best practices. The policy also requires the separation of development/test environments from production environments, and restriction of production data for testing or development.

The Change Management Policy is communicated to relevant personnel and updated annually, or as business needs require. The Compliance Team is the owner of the Change Management Policy, responsible for ensuring that changes to IT services are made in a manner appropriate to their impact on Company Operations.

Data Backup and Disaster Recovery

BriefCatch never stores or retains customer document data. The data backup and restoration policy includes every BriefCatch 3 database. Automated tools are used to achieve

daily backups, and access to backups is limited to privileged users. The ability to restore data from backups must be tested at least once a year through actual test restores.

BriefCatch has a Disaster Recovery Plan that is tested whenever significant changes to procedures invalidate prior tests, ensuring preparedness in the event of a disaster. The plan involves communicating with the entire organization, declaring a disaster state, assessing damage, determining acceptable delay times for service resumption, and providing employees with the necessary tools for prompt and effective role performance. To keep backup documentation up to date, the Compliance Team is responsible for performing an annual review.

Encryption

All connections to and from BriefCatch utilize encryption through TLS 1.2/1.3, ensuring the highest level of security and data integrity during transmission.

Incident Response

BriefCatch relies on the incident logging systems for incidents impacting cloud services such as Google Cloud Platform, Amazon Web Services, and Microsoft Azure. For other incidents, incident response guidelines are published and available to all employees and include definition of an incident, employee responsibilities and notification procedures, and data necessary to analyze an incident to determine and document the impact. A security incident recovery test is performed annually; resulting findings are integrated into the Security Incident Response Plan.

The Security Incident Response Plan includes:

- Definition of an incident
- Employee responsibilities
- Notification procedures
- Containment
- Mitigation plan
- A step to apply patch, fix, restoration of data, or enable new tool setting (such as firewall rules)
- Restoration of services
- Root cause analysis

A tracking system is in place to centrally maintain, manage, and monitor change requests that result from incidents that require a change to be made. Incident response procedures for all employees are included in the annual security training.

Incidents in the Last 12 Months

There have been no reported incidents in the 12 months prior to the end date of the audit period covered by this report.

Security Awareness

BriefCatch provides awareness training to all employees and contractors on relevant topics such as cybersecurity, data protection, and regulatory compliance. This ensures that all individuals understand the risks associated with their role and are aware of the latest best practices.

Security Management

Management has developed information security policies and related procedures to govern the security program at BriefCatch. The Information Security Policy is maintained, reviewed, and annually updated by the Compliance Team. The development of an information security program, processes, and procedures are the responsibility of the Compliance Team. The Information Security Policies are reviewed and approved annually or as business needs change. Procedure documents related to access control and change management are updated as business needs change.

These policies and procedures cover the following key security life cycle areas:

- Data classification
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response

System Monitoring

BriefCatch 3 is monitored on both the infrastructure level and the application level.

By default, Google Cloud Platform, Amazon Web Services, and Microsoft Azure provide several virtualized layers of security and antivirus within their respective platforms. At the infrastructure level, cloud automated tools within Google Cloud Platform, Amazon Web Services, and Microsoft Azure are used to monitor BriefCatch 3 performance and detect abnormalities, as well as log changes to cloud services which are audited on an as-needed basis. Notifications are monitored by the IT Team and all critical alerts will contact appropriate members through a combination of email, text, and/or voice messages.

Antivirus protection is configured on all company-issued devices to prevent the accidental or intentional malicious introduction of issues into the environment.

Controls provided by Subservice Organizations

BriefCatch 3 uses cloud services provided by three subservice organizations: Google Cloud Platform, Amazon Web Services, and Microsoft Azure (Microsoft Azure). These cloud services are used to host and manage various aspects of the System, including storage, processing, communication, and security. The subservice organizations are evaluated to ensure they align with BriefCatch's security and compliance requirements.

In order to maintain the security and availability of the BriefCatch 3 application, subservice organizations provide the following controls:

- Access controls to restrict access to data and systems to only authorized personnel. This includes implementing strong passwords, multi-factor authentication, and role-based access controls.
- Network security controls including antivirus, firewalls, and automated intrusion detection and prevention tools, to protect against unauthorized access and data breaches.
- Data Encryption controls to protect data at rest and in transit using encryption algorithms such as Advanced Encryption Standard (AES) and Transport Layer Security (TLS 1.2+).
- Monitoring and Logging controls to detect and investigate security incidents. This includes logging system activity, monitoring access logs, alerts, and reviewing logs for suspicious activity.
- Physical Security controls to protect against physical threats, such as theft, vandalism, and natural disasters. This includes implementing access controls to data centers, security cameras, and security personnel.

Incident Management processes to ensure timely detection, reporting, and response to security incidents. This includes conducting regular security audits, implementing intrusion detection and prevention systems, and an incident response plan.

Compliance and Auditing controls to ensure they comply with regulatory requirements and standards. This includes undergoing regular security audits and assessments and providing customers with relevant compliance certifications and reports.

By using subservice organizations that provide these controls, BriefCatch 3 is able to benefit from their advanced cloud infrastructure and services while maintaining a high level of security and availability. BriefCatch maintains a list of the subservice organizations used to support the System, which is regularly updated and reviewed.

Vendor Management

The organization clearly defines vendor contract expectations and vendor risks in adherence to the Vendor Management Policy. Vendor management is overseen by the Compliance Team. Formal contracts are utilized for vendor and business partner relationships; scope, responsibilities, compliance requirements and service levels (where required) are included in the contracts.

BriefCatch performs due diligence activities over new vendors prior to contract execution and on an annual basis thereafter. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk. Third party SOC 2 reports may be reviewed for impact to the company environment.

We’re here to help!

For questions, please contact us at help@briefcatch.com.