BENCHLY

Security and Data Protection Whitepaper

Benchly, Inc.

June 10, 2025

Table of Contents

Executive Summary

We deeply value the trust our customers place in us, and protecting their personal and sensitive information is at the heart of everything we do. Knowing how important data protection is, we've created strong privacy and security practices to keep our customers' information safe. Our commitment to security and privacy touches every part of our operations. We're also dedicated to being transparent, ensuring our customers always understand how their data is managed and protected.

This document consolidates essential technical, compatibility, security, privacy, and data protection information within the Benchly ecosystem, while incorporating high-level insights from our SOC 2 Type II compliance report.

Company Overview

Founded in 2016 by a team of legal technologists, Benchly was established through the acquisition of a comprehensive U.S. case law database. While this database serves as the foundation for advanced legal research, Benchly extends its capabilities further, creating litigation support tools such as the Benchly Table of Authorities Generator, purpose-built to streamline document drafting and review workflows. This approach positions Benchly as a fully independent solution, eliminating reliance on third-party database maintenance or data-sharing practices to perform intricate legal tasks efficiently.

Benchly’s mission centers on providing solutions that are simple to understand, easier to use, and less cost-intensive than our high-priced counterparts. Benchly offers the most comprehensive and technologically advanced solutions of its kind with the commitment to never cease optimizing these solutions for the betterment of our clients’ experiences.

Contact Information

Benchly, Inc.
1773 Westborough Drive
Katy, TX 77449
+1 281-293-9900
http://www.benchly.com
info@benchly.com

What is Benchly?

Benchly's Table of Authorities Generator is a comprehensive document review and Table of Authorities generation platform that improves accuracy, increases efficiency, and significantly reduces error occurrences in litigation documents.

The Benchly add-in functions as an on-premises COM/VSTO application, deployed to user workstations via an EXE or MSI file. Designed with a strict focus on data privacy, our add-in operates locally, isolating and extracting only the published citations within the user's document. This precise approach ensures that no other content is accessed or captured, reinforcing stringent privacy standards and minimizing data exposure by eliminating any need for external data transmission or storage.

System Requirements

1. Operating System
    - Windows 10+
2. Microsoft Word Version
    - Microsoft Word 2016 (Office 2016 or later)
    - Architecture: 64-bit MS Word architecture required
3. Additional Requirements
    - Permissions: Administrator rights required for installation
    - Network: Internet connection required for installation, updates, initial login, and Confirm Citations operation

Microsoft Security Compliance

Benchly strictly adheres to Microsoft's security standards for COM add-ins, ensuring a secure, reliable experience for users within the Microsoft Word environment. By leveraging Microsoft's robust framework, the add-in operates in a sandboxed environment that isolates its processes, protects user data, and minimizes risks to the system. This commitment to security means that all data processing remains localized, with strict controls in place to align with Microsoft's privacy and performance requirements. As a Microsoft Word COM Add-in, Benchly adheres to Microsoft's stringent security requirements for COM add-ins, providing a secure, user-focused experience that prioritizes data privacy and integrity.

Architecture

The Benchly add-in is deployed via EXE or MSI files to ensure direct installation on user workstations. Once installed, it operates within a 64-bit Microsoft Word environment, leveraging Microsoft's COM add-in framework for compatibility and security.

Risks & Vulnerabilities

As with any Office add-in, potential risks include unauthorized access to system resources and data exposure. Benchly mitigates these risks by adhering to Microsoft's security protocols, which involve isolating the add-in's runtime processes and limiting access to system resources.

Preventative Measures

- User Confirmation for Sensitive Actions: Benchly incorporates user confirmation dialogs for distinct operations, ensuring users are fully informed before any action is taken within their document, reducing the risk of unauthorized activity.
- Secure Display Outside the Add-In Context: For critical confirmations, the add-in utilizes secure prompts outside the primary add-in frame, preventing hidden or manipulated actions by malicious actors within the interface.
- Verified Contact Methods: Benchly uses only pre-verified contact methods for user confirmations, ensuring any sensitive communications are directed at secure, authorized channels.

Security Compliance Measures

The Benchly add-in follows Microsoft's compliance standards for Office add-ins, which include:

- Access Control: Restricting add-in access to the Office application's UI and limiting permissions to prevent unauthorized interactions.

- Process Isolation: Isolating the add-in's process, which prevents interference with the main Office application or other add-ins.
- Resource Management: Governing memory, CPU, and network resource usage to ensure reliability and prevent performance issues.

Sandbox Environments

The add-in's runtime environment runs within a secure, sandboxed process on the local workstation, isolating its operations from the main application. This design prevents unauthorized system access or data breaches by restricting the add-in's permissions and interactions within the host application.

Promotion of End User Security Controls

The Benchly add-in was developed with Microsoft's security and compliance standards as core considerations, ensuring a secure, reliable experience for end users. Key controls incorporated into the design include:

- Compatibility Awareness and Security Preparation: The Benchly add-in was developed with Microsoft's compatibility and security standards in mind, ensuring seamless integration and robust security for end users.
- Avoidance of ActiveX Controls: By intentionally avoiding unsupported ActiveX controls, the add-in maintains compatibility and reliability within the Office environment.
- Enable/Disable Trace Logging: Provides end users with the option to enable or disable trace logging, allowing for detailed activity logs to be generated selectively to assist in troubleshooting and efficiently resolving support queries, while minimizing unnecessary data collection.
- Privacy Policy Alignment: A compliant privacy policy outlines Benchly's data handling practices, upholding transparency and meeting Microsoft's privacy standards. Benchly's Privacy Policy is available at https://www.benchly.com/privacy-policy

End User's Perspective

From the end user's standpoint, Benchly functions like a standard Office tool, with most data processing securely handled on their local machine. An exception occurs during the optional Confirm Citations operation, where published citations in the user's document are cross-referenced with the Benchly case law database. Privacy and security are reinforced by limiting data handling strictly to relevant citations, ensuring that users' content remains untouched and their data secure. Additionally, the add-in requires user permission on initial use, aligning with Microsoft's policy of informed consent.

SOC 2 Type II Report Compliance Journey

Benchly achieved SOC 2 Type II compliance in April 2025, reinforcing our commitment to securing user data and meeting the highest industry standards. This certification, issued by an independent AICPA-certified auditor following a rigorous six-month control review, verifies that our systems and processes consistently protect client information across security, availability, processing integrity, confidentiality, and privacy. As part of AICPA standards, Benchly's SOC 2 Type II controls are evaluated annually to ensure continued effectiveness and compliance. The full report is available upon request and will be distributed once a non-disclosure agreement (NDA) between Benchly and the requestor's organization has been executed. Visit www.benchly.com/trustcenter for more information.

Purpose of SOC 2 Type II Report

The purpose of a SOC 2 Type II report is to validate an organization's commitment to data privacy and security through rigorously tested controls. This independent assessment confirms that systems meet high standards for protecting sensitive information, particularly in data privacy, confidentiality, and availability. The core advantage of SOC 2 Type II is its role in building client trust, demonstrating that an organization has robust, consistently applied safeguards in place.

Phases of the SOC 2 Type II Compliance Process

1. Risk Assessment and Gap Analysis: Identified control gaps against SOC 2 standards, laying a roadmap for technical improvements.
2. Control Implementation: Rolled out access, encryption, monitoring, and incident response controls tailored to SOC 2's Trust Service Criteria.
3. Monitoring and Pre-Audit Review: Continuous monitoring and internal audits ensure ongoing compliance readiness. (Engagement letter available on request only).
4. Independent SOC 2 Audit: Partnering with an AICPA-certified auditor validates our control effectiveness over an extended evaluation period.
5. Completion of audit and awaiting SOC 2 Type II Report.
6. SOC 2 Type II Report obtained with annual control audits recurring.

Data Privacy and Flow

Benchly is committed to data privacy by collecting only the minimal information necessary to achieve functionality. Benchly further isolates specific data within a user's document, processing only what is required for formatting and Table of Authorities generation. This approach ensures minimal data exposure and secure handling, reflecting our dedication to protecting user information and content.

Minimal Data Collection Approach

Benchly employs a minimal data collection approach to prioritize user privacy and reduce data handling to the absolute essentials. For license allocation, we require only the following of the end user's information:

- Company
- First Name
- Last Name
- Company email address

No additional personal information is collected or stored. Additionally, Benchly strictly isolates the published citations within a user's document, processing only this specific content to perform formatting checks and generate an accurate Table of Authorities. This targeted approach ensures that Benchly accesses only the necessary information to deliver our services, upholding privacy standards and minimizing exposure of user content.

Application Data

Application data refers to the specific information or content that the add-in accesses, generates, or modifies within Microsoft Word. This data is tied to the add-in's functionality and includes the following elements:

- User-generated Content: In the context of Benchly, the Add-in solely interacts with the citations or cited authority referenced within a document. While this content type is user-generated, citations are published references to publicly available authoritative legal sources.
- Configuration Settings: Users can create and modify format preferences that exclusively apply to the Table of Authorities and save those preferences in a Format Profiles selector. When selected, the preferences will be recalled and applied to a user's Table of Authorities to aid in complying with court formatting requirements.
- Metadata: Benchly utilizes Microsoft Word's native Table of Authorities (TA) entries, removing the need for proprietary codes to achieve functionality. This approach embeds citation data as native metadata, ensuring full compatibility with Word's formatting and review tools while preserving document integrity.

Usage Data

Benchly categorizes usage data by tracking interactions with core features, such as performing the Find operation, Table of Authorities generation, citation checking, and hyperlinking. This data is stored and is temporarily utilized solely to facilitate the add-in's essential functions alongside reporting mechanisms for license administrators and support ticket resolution solely by the Benchly Support Team, ensuring a streamlined user experience without retaining any personal metrics other than the type and number of actions a user performs.

- Frequency of Table of Authorities Generation: How often users generate or update the Table of Authorities (TOA).
- Feature Usage Patterns: Data on specific TOA-related features used, including:

Find Operation	Confirm Citations
Build TOA	Hyperlink Authorities

- Processing Time: The time taken to generate or update the TOA, which can indicate performance efficiency or inefficiencies.
- Error Occurrences: Any errors encountered while tagging entries or generating the TOA, useful for troubleshooting and improving reliability.
- Trace Logging: Users can opt to enable trace logging within Benchly to capture detailed activity logs, assisting in troubleshooting, and diagnosing issues efficiently.

This usage data supports performance optimization, feature enhancement, and targeted troubleshooting in the add-in. At times, Feature Usage Pattern data may be collected for both reporting and product improvement purposes.

Data Flow

Usage data generated by the Benchly add-in is securely stored in the user's local AppData Trace Log folder, ensuring that operational data remains confined to the user's workstation. Feature usage patterns, however, are securely recorded in Benchly's centralized activity log for reporting and monitoring. This dual storage approach ensures operational data in the user's AppData Trace Log folder stays within the user's environment, while feature usage patterns in Benchly's activity log are securely managed.

Retention and Removal

The Benchly add-in allows end users or administrators to manage retention of usage data by electing to remove or clear the AppData folder at any time, ensuring full control over data persistence. Additionally, upon uninstallation of the add-in, all related Benchly data within the AppData folder is automatically removed, guaranteeing that no residual data remains on the user's system. This approach prioritizes data security and user autonomy, aligning with best practices for data management and retention.

Technical Implementation

The Benchly add-in's technical implementation provides flexible installation options, offering both per-user and per-machine methods to support varied user and organizational requirements. This setup enables seamless integration with Microsoft Word, optimizing for security and performance across environments.

The **per-user installation**, facilitated by an EXE installer, is ideal for individual users or smaller teams. This installation method installs the Benchly add-in exclusively for the active user profile, storing relevant data and configurations within the user's AppData folder. This approach allows quick deployment without requiring administrative permissions, making it convenient for users to install and update independently while still maintaining secure, localized data handling.

The **per-machine installation**, managed through an MSI installer, is intended for enterprise environments or multiple-user workstations. This method installs the Benchly add-in for all users on the machine, requiring administrative privileges during installation. The MSI installer ensures consistent access across user profiles on a single machine, centralizing installation and updates to facilitate maintenance by IT administrators while preserving security protocols and local data storage for each user session.

Data Protection

Benchly is committed to safeguarding user data through robust technical controls and measures that align with SOC 2 report standards. Our data protection strategy includes encryption protocols for data at rest and in transit, strict access controls, and continuous monitoring to detect and respond to potential threats. These practices are reinforced by localized data storage, ensuring that operational data remains securely within the user's environment, minimizing exposure. This rigorous approach to data security demonstrates our dedication to upholding privacy and protecting user information at every level.

Encryption Standards

Benchly utilizes Azure's advanced encryption standards to protect our database and user-generated citations in transit, applying AES-256 encryption for data at rest and TLS 1.3 for data in transit. These protocols prevent unauthorized access and protect data integrity, whether stored or transmitted. Additionally, Azure's Key Vault service securely manages encryption keys with features like key rotation and access monitoring, ensuring that encryption is handled with high security at all stages. This alignment with Azure's encryption standards ensures strong protection for user data and reinforces privacy across our platform.

Change Management

Change management within Benchly's COM add-in environment is a structured process designed to ensure stability, security, and data integrity with each update or modification. All proposed changes undergo a rigorous review process, including code testing, security analysis, and impact assessment to verify compatibility within Microsoft Word and adherence to our minimal data collection approach. By implementing a controlled change management workflow, Benchly ensures that each alteration supports optimal functionality without compromising the security of user environments or data privacy.

Each change is systematically tracked and documented, with detailed logs capturing the nature, rationale, and results of modifications. This documentation provides a clear audit trail, allowing us to trace each update and identify any potential issues that may arise post-deployment. For our COM add-in, which operates locally on the user's workstation, this level of documentation is crucial to maintaining transparency and ensuring each change aligns with Microsoft's security standards while respecting our minimal data collection approach by preserving only essential user information.

Data Backup and Disaster Recovery

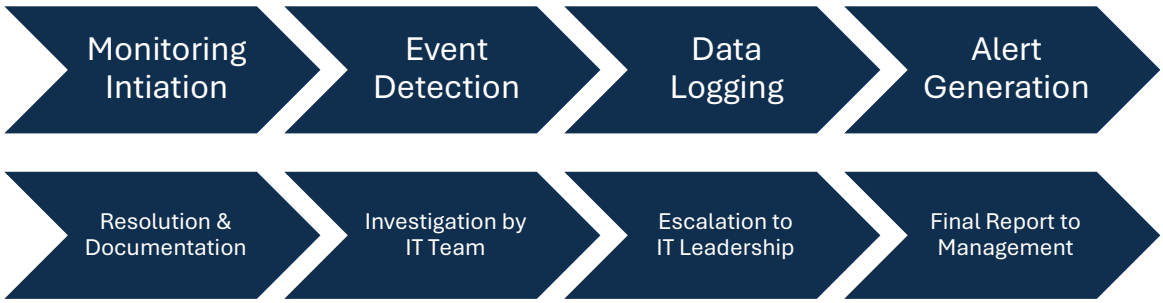
Benchly prioritizes data resilience through regular, secure backups stored within Microsoft Azure's highly reliable cloud infrastructure. By leveraging Azure's advanced security measures, including encryption, multi-factor authentication, and extensive physical and network safeguards, we ensure that all backed-up data remains protected and recoverable in the event of an incident. These backups are automatically replicated across multiple Azure data centers, enhancing both data availability and durability. Through Azure's robust compliance with industry standards and security controls, Benchly provides users with reliable data protection and swift recovery capabilities, reinforcing our commitment to data integrity and continuity.

Benchly has established a comprehensive Disaster Recovery Plan (DRP) to ensure the continuity and resilience of our operations in the event of unexpected disruptions. The plan includes clearly defined communication channels, detailed roles and responsibilities for each team member, and a structured disaster response team hierarchy to streamline decision-making and response actions. This coordinated approach enables us to respond rapidly and effectively to potential incidents, protecting data integrity and minimizing downtime.

Our Disaster Recovery Plan is available upon request.

System Monitoring

Our internal system monitoring process is structured to ensure real-time oversight and swift resolution of any issues that may impact functionality, security, or user experience. Monitoring begins with automated event detection and data logging, capturing relevant activity to identify potential access issues, bugs, or performance bottlenecks. If a significant event is detected, alerts are generated and reviewed by the IT team. This structured approach allows us to investigate and resolve issues promptly, documenting each step for accountability and continuous improvement. All logged information is securely retained, enabling us to address specific access concerns, troubleshoot bugs, and identify opportunities for feature enhancements that support ongoing system optimization.



Proactive Monitoring

Benchly's proactive monitoring for our COM add-in is designed to identify and address potential issues before they impact user experience or system security. By continuously tracking key performance metrics and setting automated alerts for specific thresholds, our team can detect anomalies early and take preventive action. Regular security audits and capacity planning further ensure that the add-in remains stable and responsive as user demand grows, safeguarding the add-in's performance within Microsoft Word and maintaining a smooth, reliable experience.

Reactive Monitoring

Benchly's reactive monitoring approach enables rapid incident response within our COM add-in, reducing downtime and user disruption. When issues arise, structured response protocols and real-time alerts allow our team to act quickly, while error tracking and root cause analysis help resolve the problem at its source. Each incident is documented to contribute insights that enhance the resilience and reliability of our add-in, ensuring ongoing improvement and robust functionality for our users.

Vendor Management

Before onboarding any new vendors, we conduct thorough due diligence to ensure they meet our stringent security standards. This process involves evaluating each vendor's information security practices, examining their policies, and assessing their ability to safeguard sensitive data. By thoroughly vetting potential vendors, we establish a strong foundation of trust and alignment with our commitment to data protection.

In addition to initial evaluations, we maintain continuous oversight of our vendor relationships to uphold high security standards. Regular reviews and assessments are conducted to verify that vendors remain compliant with our security protocols and practices. Through these scrutinous measures, we ensure that our users' data remains protected, reinforcing our commitment to privacy and security in every aspect of our operations.

Subservice Organizations

Benchly has selected Microsoft Azure as our data storage partner. Microsoft Azure's approach to compliance is rooted in a robust system of assurances that reinforce security and regulatory alignment. This includes a variety of independent third-party audits, such as certifications, attestations, and authorizations, as well as validations and assessments, all conducted by trusted auditing organizations. These third-party measures ensure that Azure's infrastructure meets the highest standards across multiple industries.

Beyond external audits, Microsoft provides additional compliance tools, including tailored contractual amendments, internal self-assessments, and comprehensive customer guidance resources. These tools offer clear, practical support to help clients achieve and maintain compliance within Azure's cloud framework. Azure's compliance program addresses diverse regulatory requirements, reflecting Microsoft's dedication to a secure and compliant environment for its users.

Microsoft Azure Security Certificates/Reports	
SOC 1	ISO 27001
SOC 2	ISO 27017
SOC 3	ISO 27018
ISO 20000	ISO 27701
ISO 22301	CSA STAR Levels 1-3

Addressing Government-Specific Security Concerns

Benchly is dedicated to meeting the rigorous security standards required by government agencies, ensuring that sensitive data is protected with industry-leading safeguards. In addition to obtaining our SOC 2 Type II report, we are TX-RAMP Level 2 certified, underscoring our commitment to compliance with stringent state and federal data protection regulations. These certifications reflect our adherence to strict privacy, confidentiality, and availability standards, providing government clients with the assurance that their information is handled with the highest level of care.

With a proven track record of successful collaborations with major government agencies, Benchly has demonstrated a thorough understanding of the unique security requirements and compliance needs specific to the public sector. Our systems and protocols are designed to uphold these standards reliably, from data encryption and access control to regular audits and continuous monitoring. This commitment enables us to support government clients in maintaining data security while aligning with complex regulatory requirements.

Conclusion

In conclusion, Benchly's dedication to robust security and privacy is demonstrated across all facets of our platform, from our SOC 2 Type II compliance achievement to our stringent adherence to Microsoft's security standards for COM add-ins. As an organization rooted in providing secure, efficient tools for legal and government sectors, we uphold rigorous data protection measures, including encryption, controlled data flow, and minimal data collection to prioritize user privacy.

Through our carefully structured technical implementation, Benchly's add-in integrates seamlessly with Microsoft Word, providing users with a powerful, secure solution that is purpose-built to optimize Table of Authorities generation. Our commitment extends to proactive change management, regular data backups, and a comprehensive disaster recovery plan, ensuring resilience and continuity. In alignment with the high standards expected by government agencies, our TX-RAMP Level 2 certification further demonstrates our commitment to addressing specialized security requirements.

With secure system monitoring, thorough vendor management, and collaboration with a trusted subservice provider, Benchly maintains a secure, compliant environment that meets the complex needs of our clients. This multi-layered approach reflects our mission to support legal professionals with secure, dependable technology tailored to the highest standards of data protection and privacy.