Strike Labs Security Best Practices

A Comprehensive Framework for Every Product

Updated as of 10/27/2023

Welcome

At Strike Labs, security is not merely a priority; it is an immutable cornerstone ingrained into the very fabric of our operations. We recognize that in the complex landscape of modern technology, security is not a one-size-fits-all endeavor. Instead, it's an intricate tapestry woven with threads of vigilance, expertise, and unwavering dedication. We understand that the nature of security transcends one-dimensional approaches; it's a multi-faceted realm where diverse levels of protection, clearances, and compliance considerations converge.

In this extensive document, we embark on a journey through the core of our security ethos. We delve into the intricate web of security best practices that form the bedrock of every product we conceive and deliver. Our commitment to security extends far beyond the superficial; it is a profound philosophy that defines our mission, encapsulates our values, and ultimately ensures that every solution we create adheres to the loftiest standards of protection.

1. **Understanding Security at All Levels** - At Strike Labs, we comprehend the diverse dimensions of security, recognizing that it encompasses much more than a mere checklist of requirements. Security, in its true essence, is an ecosystem where every element is carefully orchestrated to fortify the whole. From the intricate web of user validation to the robust fortifications against unauthorized access, from the impervious shield of data security to the meticulous disaster recovery measures, every facet plays a crucial role in ensuring the sanctity of the digital realm.
2. **Clearance and Compliance** - Furthermore, we are keenly aware that the security landscape is not monolithic. Different sectors, industries, and organizations have unique clearance requirements and compliance obligations. Our security practices are not confined by boundaries; instead, they are adaptive and scalable, tailored to meet the exacting demands of federal clients, the healthcare sector under HIPAA, the financial realm guided by GLBA, the protection of children's data under COPPA, and the broader consumer protection and privacy standards enforced by the FTC. We understand that security must be as dynamic as the environments it safeguards.
3. **An Invitation to Learn More** - This comprehensive document serves as a testament to our unwavering commitment to security. It is not just a statement of intent but a detailed exploration of how we operationalize security in every product we create. We invite you to journey with us through the intricate security tapestry that

defines Strike Labs. By understanding our practices, you gain insights into the depth of our dedication to protecting your interests and data.

4. **A Recommendation for Consideration** - Moreover, as we unveil the layers of our security framework, we do so with a broader perspective in mind. We recommend that, beyond learning about our practices, you consider the same level of scrutiny for security in your own endeavors. In an interconnected world where data is the lifeblood of operations, security is not just a choice; it is an imperative. The lessons learned from our approach can be valuable in fortifying your own digital citadel, ensuring the sanctity of your data, and upholding the trust of your stakeholders.

This document is not merely a compendium of practices; it is a testament to our unwavering commitment to security excellence. We stand ready to provide you with beautiful, secure software development solutions that align with your mission and data protection needs. As you embark on this journey with us, may you find inspiration, insights, and a shared commitment to elevating security to the highest priority.

Table of Contents

User Validation

User validation serves as a pivotal pillar within our security framework, meticulously confirming the identities of individuals seeking access to systems, platforms, or applications. It assumes a foundational role in guaranteeing that only authorized and legitimate users gain entry to sensitive data, services, or resources.

At Strike Labs, our dedication to user validation transcends the boundaries of a singular regulatory framework. Instead, it embraces a multifaceted approach meticulously crafted to align with the stringent demands set forth by GDPR, CCPA, HIPAA, GLBA, COPPA, and FTC regulations. This holistic strategy harnesses advanced techniques and verification mechanisms to fortify the authenticity of user identities, reinforcing the protective fortifications of our security framework against any encroachments by unauthorized entities.

Email Verification

During the initial stages of user registration, we mandate a rigorous email verification process. This involves the issuance of a cryptographically secure, one-time token or link sent to the provided email address. By clicking the link or entering the token, the user's email is confirmed, thus validating the authenticity of their account. This practice aligns with GDPR and CCPA requirements for secure data processing and user identity verification.

Example: A unique verification link, cryptographically signed for security, is sent to the user's email address upon registration. Clicking on this link verifies their email, ensuring compliance with GDPR and CCPA data protection principles.

Phone Verification

In line with CCPA, HIPAA, and FTC guidelines, we incorporate phone number verification as an additional layer of validation. This process necessitates the confirmation of phone numbers through SMS or voice verification. By implementing this stringent measure, we significantly mitigate the risk of unauthorized access, thereby safeguarding sensitive information.

Example: After registering, users receive a text message containing a one-time verification code or a phone call for voice verification. Entering the code or confirming the call authenticates their phone number and enhances the security of their account, aligning with CCPA, HIPAA, and FTC standards.

Identification Documents

For scenarios demanding the highest level of identity verification, we have the capability to request government-issued identification documents, such as driver's licenses or passports. This practice aligns with HIPAA and GLBA requirements for robust identity validation, especially in healthcare or financial contexts.

Example: In situations where regulatory compliance is paramount, users may be prompted to securely upload scans of their government-issued IDs, ensuring compliance with HIPAA and GLBA privacy and security standards.

Knowledge-Based Questions

In strict adherence to CCPA, COPPA, and FTC regulations, we leverage knowledge-based questions derived from a variety of data sources, including credit reports and public records. These inquiries challenge users with specific, non-trivial questions about their personal history, strengthening identity verification.

Example: During high-security interactions or account recovery processes, users might be presented with questions like, "Which of the following addresses have you lived at in the past five years?" based on data from credit reports, aligning with CCPA, COPPA, and FTC guidelines.

User Self-Service Security Settings

Empowering users to take control of their security is at the core of our approach. Within their accounts, users have the autonomy to configure self-service security settings, encompassing options for password changes and the setup of multi-factor authentication (MFA). This proactive approach allows users to tailor their security preferences, aligning with the data protection principles of GDPR, CCPA, HIPAA, GLBA, COPPA, and FTC.

Example: In their account settings, users can enable MFA by selecting their preferred authentication method, such as a time-based one-time password (TOTP) or hardware token, thus aligning with the stringent security standards of all applicable regulations.

By meticulously implementing this comprehensive suite of identity verification measures, Strike Labs ensures the highest level of compliance not only with GDPR but also with CCPA, HIPAA, GLBA, COPPA, and FTC regulations. This unwavering commitment to rigorous identity verification is a testament to our dedication to safeguarding sensitive information, meeting the unique demands of each regulatory landscape, and maintaining the integrity of our security framework.

Unauthorized Access Prevention

Unauthorized Access Prevention stands as a pivotal facet of security, diligently crafted to thwart any attempts by unauthorized individuals or entities to breach the sanctity of sensitive data, systems, or organizational resources. Its foremost objective is the establishment of formidable defenses and mechanisms, rendering unauthorized entry or usage an insurmountable challenge. In doing so, it guarantees that only duly authorized personnel or entities are granted access to safeguarded assets.

Within the realm of Strike Labs, our unwavering commitment to unauthorized access prevention takes shape as a multifaceted strategy. It not only harmonizes with the stringent mandates of GDPR but also embraces the formidable data security requisites stipulated by CCPA, HIPAA, GLBA, COPPA, and the vigilant oversight demanded by the FTC. Our comprehensive array of measures is meticulously designed to reinforce our products against a diverse spectrum of threats, thus upholding the paramount principles of data security and user privacy across a multitude of regulatory landscapes.

Multi-Factor Authentication (MFA)

Enforced for every product we develop, MFA is a cornerstone of our defense against unauthorized access. This advanced authentication mechanism requires users to provide multiple forms of verification, such as something they know (password) and something they have (security token), or something they are (biometric data). This practice aligns with GDPR's mandate for robust authentication and is equally critical for CCPA, HIPAA, GLBA, and FTC compliance.

Example: Users are required to enter their password and a time-based one-time password (TOTP) generated by an authentication app to gain access, enhancing security in accordance with multiple regulations.

Biometric Verification

To meet the stringent demands of data protection policies, we offer biometric verification options, including fingerprint or facial recognition. Biometric data is a highly secure form of authentication, aligning with the heightened security expectations of HIPAA and the comprehensive protection required by CCPA and

GLBA.

Example: Users can opt to use fingerprint or facial recognition to unlock their accounts, providing a high level of security and compliance with HIPAA, CCPA, and GLBA.

IP Address and Geolocation Verification

Our systems incorporate IP address and geolocation verification to ensure that users are accessing our products from authorized locations. This measure aligns with GDPR's emphasis on controlling access based on geographical restrictions and is critical for maintaining the privacy and security of user data under CCPA, HIPAA, and GLBA.

Example: If a user attempts to access their account from an unfamiliar location, our system may trigger an additional authentication step to confirm their identity, in compliance with multiple regulations.

Device Fingerprinting

Recognizing registered devices through advanced technology is an integral part of our access control strategy. This technique adds an additional layer of security by identifying devices and ensuring that only authorized devices can access sensitive data. This is essential for complying with the access control requirements of GDPR, CCPA, HIPAA, and GLBA.

Example: Each device accessing our platform is assigned a unique device fingerprint. If a device with an unrecognized fingerprint attempts to log in, additional verification steps may be triggered to prevent unauthorized access.

CAPTCHA and Bot Detection

GDPR encourages protection against automated attacks, and we achieve this through the implementation of CAPTCHA challenges and advanced bot detection mechanisms. This ensures that only human users can access our systems, in compliance with GDPR, CCPA, and the FTC's expectations for safeguarding against deceptive practices.

Example: When our system detects suspicious behavior consistent with automated bots, it presents a CAPTCHA challenge to verify the user's humanity, thereby aligning with multiple regulatory standards.

Stringent Password Rules

Our enforcement of strong password rules is in strict adherence to GDPR's data security principles. This includes requirements for password complexity, length, and regular expiration. Password security is vital for safeguarding data under CCPA, HIPAA, and GLBA.

Example: Users are required to create passwords that meet specific complexity criteria, including a mix of uppercase and lowercase letters, numbers, and special characters, to ensure compliance with multiple regulations.

Automatic Account Lockout

In compliance with data protection regulations, we have implemented an automatic account lockout mechanism. This temporarily locks accounts after detecting suspicious activity or a specified number of failed login attempts. This practice ensures data security and aligns with GDPR, CCPA, and HIPAA.

Example: If a user attempts multiple unsuccessful login attempts or exhibits suspicious behavior, their account is automatically locked for a predetermined time, bolstering security in accordance with multiple regulatory frameworks.

Session Management

Idle timeout mechanisms are integral to our access control strategy. These mechanisms automatically log users out after a period of inactivity, preventing unauthorized access. This practice aligns with GDPR's emphasis on session control and is equally relevant for CCPA, HIPAA, and GLBA compliance.

Example: If a user remains inactive for a specified period, our system terminates their session and requires reauthentication, ensuring compliance with multiple regulations.

User and Entity Behavior Analytics (UEBA)

Our systems are equipped with UEBA capabilities, enabling the detection of unusual behavior patterns. This aligns with GDPR's requirement for continuous monitoring and threat detection. UEBA is essential for safeguarding data under CCPA, HIPAA, and GLBA.

Example: Our UEBA tools analyze user behavior patterns and can trigger alerts for abnormal activities, such as unauthorized access attempts, aligning with multiple regulatory expectations.

By implementing these advanced access control measures, Strike Labs not only aligns with the rigorous standards of GDPR but also goes beyond to meet the demands of CCPA, HIPAA, GLBA, COPPA, and the FTC. This unwavering commitment to unauthorized access prevention ensures that data security and user privacy remain paramount in an evolving regulatory landscape.

Data Security

Data Security represents a holistic collection of practices, cutting-edge technologies, and meticulous measures meticulously orchestrated to shield digital data from any encroachments in the form of unauthorized access, disclosure, tampering, or obliteration.

At Strike Labs, our unwavering commitment to data security transcends the mere confines of GDPR and extends harmoniously to embrace the stringent data protection imperatives delineated by CCPA, HIPAA, GLBA, COPPA, and the vigilant oversight expected by the FTC. Our data security protocols are ingeniously engineered to furnish all-encompassing guardianship to data assets, effortlessly spanning the diverse tapestry of regulatory landscapes, all while leveraging avant-garde technologies and methodologies.

End-to-End Encryption

Our data security begins with end-to-end encryption. All data transmitted within our network, whether it's user communications, sensitive documents, or transaction data, is encrypted using strong cryptographic algorithms. This practice aligns with GDPR's emphasis on protecting data during transmission and is essential for CCPA, HIPAA, and GLBA compliance.

Example: When a user sends a confidential message through our platform, it is encrypted at the sender's end and decrypted only at the recipient's end, ensuring that data remains confidential in transit.

Encrypted at Rest

Data stored on our servers is encrypted at rest, adding an additional layer of security. This means that even if an unauthorized party gains physical access to our servers, the data remains protected. This measure is crucial for safeguarding sensitive information under CCPA, HIPAA, and GLBA.

Example: When user data is stored on our servers, it is stored in an encrypted format, rendering it unreadable without the proper decryption keys.

Role-Based Access Control (RBAC)

We employ RBAC to efficiently manage user access and permissions. This practice ensures that users only have access to the data and functionalities necessary for their roles. RBAC aligns with GDPR's need for role-based data access and is pivotal for compliance with CCPA, HIPAA, and GLBA.

Example: A healthcare professional accessing our platform is granted access only to patient records and medical data relevant to their role, as defined by RBAC rules.

Access Logging and Monitoring

Comprehensive access logs and continuous monitoring are integral components of our data security strategy. These logs record all user activities and access attempts. Continuous monitoring allows us to promptly detect and respond to security threats, meeting GDPR's requirements for data auditability and supporting CCPA, HIPAA, and GLBA compliance.

Example: Our system generates detailed logs of user actions, including logins, data access, and changes made. This information is monitored in real-time for any suspicious activities.

Intrusion Detection and Prevention System (IDPS)

Real-time threat detection and mitigation are central to our data security posture. Our IDPS actively monitors network traffic and system behavior to identify and respond to potential threats. This proactive approach preserves data integrity, addressing a key concern under GDPR and safeguarding data under CCPA, HIPAA, and GLBA.

Example: If our IDPS detects an unusual pattern of network traffic that could indicate a cyberattack, it immediately triggers automated responses to mitigate the threat.

Security Information and Event Management (SIEM)

GDPR's mandate for security event data analysis is met through our SIEM tools. SIEM solutions aggregate and analyze security event data, helping us identify and respond to security incidents swiftly and comprehensively.

Example: SIEM tools correlate information from various sources, such as access logs, authentication logs, and IDPS alerts, to provide a holistic view of the security landscape.

Data Level Privacy

We implement data-level privacy controls to ensure that sensitive information is protected according to the highest standards. This includes mechanisms to restrict access to specific data elements based on user roles and permissions. Data-level privacy is a central requirement under GDPR and is equally important for CCPA, HIPAA, and GLBA.

Example: Patient records may have specific data-level privacy controls in place to restrict access to sensitive medical information to only authorized healthcare professionals.

Zero Trust Architecture

Our architecture aligns with the zero-trust model, where trust is never assumed, and verification is a prerequisite for data access. This approach is consistent with GDPR's principles and equally applicable to CCPA, HIPAA, GLBA, and FTC regulations.

Example: Even when a user is logged in, our system continuously monitors their activities and may prompt for additional verification if suspicious behavior is detected.

Data Masking and Redaction

To comply with GDPR's data minimization principles, we employ data masking and redaction techniques. Sensitive data is masked or redacted, even for authorized users who do not require access to the full dataset.

Example: Social security numbers in documents may be redacted for all users except those with explicit permissions to view them.

User Authentication Logs

We maintain comprehensive authentication logs, recording all user login and authentication activities. These logs support GDPR's requirements for data accountability and transparency and are essential for compliance with CCPA, HIPAA, GLBA, and FTC expectations.

Example: Every authentication attempt, including successful logins and failed login attempts, is logged with a timestamp and associated user information for audit and accountability purposes.

By meticulously implementing these advanced data security practices, Strike Labs not only surpasses the requirements of GDPR but also aligns with the stringent standards set by CCPA, HIPAA, GLBA, COPPA, and the FTC. This unwavering commitment to data security ensures the utmost protection for sensitive information and user privacy, regardless of the regulatory landscape.

Disaster Recovery and Data Backup

Disaster recovery represents an intricate framework of meticulously devised procedures, meticulously crafted policies, and cutting-edge technologies, all aimed at orchestrating the resuscitation of critical systems, applications, and data to an operational state following the occurrence of a catastrophic event or any disruptive incident. The primary and overarching objective of disaster recovery remains the minimization of downtime, data loss, and the perturbations to business operations in the wake of unforeseen calamities, encompassing natural disasters (e.g., earthquakes, hurricanes), cyber incursions, hardware malfunctions, or other unpredicted contingencies.

Nestled within the broader sphere of disaster recovery, data backup emerges as a dedicated subset with a laser focus on the replication of essential data and information, typically executed at regular intervals. This proactive maneuver stands as a bulwark against the specter of data loss, assuring that, in the event of data corruption, inadvertent deletion, hardware incapacitation, or cyber incursions, organizations retain the ability to restore their data to a prior state.

At Strike Labs, our approach to disaster recovery and data backup is engineered to align not only with GDPR but also with the rigorous business continuity and data availability requirements of CCPA, HIPAA, GLBA, COPPA, and the vigilance expected by the FTC. Our practices are designed to ensure the preservation, availability, and integrity of data even in the face of catastrophic events.

Off-Site Backups

Our disaster recovery strategy involves secure off-site backups that guarantee data preservation. This practice aligns with GDPR's critical need for data availability in case of disasters. These backups are stored in geographically separate, highly secure data centers or cloud environments to mitigate the risk of data loss due to physical events.

Example: A real-time backup of critical data is replicated to a geographically distant data center, ensuring that data remains accessible even if the primary data center experiences an outage or disaster.

Catastrophic Event Handling

We maintain well-defined procedures and contingency plans to address catastrophic events promptly. This includes a comprehensive disaster recovery plan that outlines steps for mitigating the impact of disasters, such as natural disasters, cyberattacks, or infrastructure failures. This approach aligns with GDPR's emphasis on disaster preparedness and is crucial for compliance with CCPA, HIPAA, GLBA, and FTC expectations.

Example: In the event of a natural disaster, our disaster recovery team is activated, following a predefined plan to restore services from backup systems and minimize downtime.

Data Backup and Recovery

Our data backup and recovery processes are engineered to minimize downtime and data loss, ensuring data integrity remains uncompromised. This encompasses regular backups, incremental backups, and point-in-time recovery options to meet the stringent data availability requirements of GDPR, CCPA, HIPAA, and GLBA.

Example: We perform hourly incremental backups in addition to daily full backups. In case of data corruption or loss, we can restore data to a specific point in time to minimize data loss.

Redundancy and Failover

Our infrastructure includes redundancy and automatic failover mechanisms. This ensures uninterrupted service even during system failures, aligning with GDPR's requirements for system availability. Redundant components are placed strategically to ensure seamless operation.

Example: If a server or data center experiences a hardware failure, traffic is automatically redirected to redundant servers or data centers, ensuring continuous service availability.

Fully Operational Service

GDPR's demand for uninterrupted service is met through our commitment to providing a fully operational network at all times. Our systems are designed to ensure high availability, and we have failover mechanisms in place to switch to backup systems in the event of an outage.

Example: Our service-level agreements (SLAs) guarantee a high level of availability, with minimal downtime allowed for maintenance or upgrades.

By meticulously implementing these disaster recovery and data backup practices, Strike Labs not only adheres to the requirements of GDPR but also aligns with the stringent standards set by CCPA, HIPAA, GLBA, COPPA, and the FTC. This unwavering commitment to business continuity and data availability ensures that critical data remains accessible, even in the face of catastrophic events, and that data integrity is preserved, safeguarding the interests of our clients and their compliance with diverse regulatory frameworks.

Redundancy and Failover

The purpose of redundancy is to eliminate single points of failure and enhance system reliability. In the event that one component fails or becomes unavailable, redundant components take over seamlessly, minimizing downtime and disruption.

At Strike Labs, our approach to redundancy and failover goes beyond ensuring uninterrupted service and aligns with the stringent system availability requirements of not only GDPR but also CCPA, HIPAA, GLBA, COPPA, and the expectations set forth by the FTC. These measures are essential for preserving data availability, maintaining service continuity, and safeguarding against system failures and disruptions.

Redundancy

Redundancy forms the foundation of our system architecture. We duplicate critical system components to align with GDPR's imperative for continuous data availability. This means having backup servers, storage systems, network infrastructure, and even power sources in place to mitigate the impact of hardware failures or unexpected outages.

Example: Our data centers are equipped with redundant power supplies, ensuring that if one power source fails, the backup source seamlessly takes over, preventing service interruption.

Failover

Automatic failover mechanisms are a key component of our strategy. These mechanisms are designed to maintain seamless operation, even during system failures. In the event of a hardware or software failure, traffic is automatically redirected to redundant components to ensure uninterrupted service.

Example: If a server experiences a hardware failure, our failover system immediately routes incoming requests to a redundant server, minimizing downtime and service disruption.

Fully Operational Service

Our commitment to providing a fully operational network aligns with GDPR's demand for uninterrupted service. We understand that downtime can have severe consequences for our clients, and we have designed our systems to minimize disruptions due to maintenance, upgrades, or unexpected issues.

Example: We have a comprehensive maintenance schedule that includes routine updates and system checks during off-peak hours to minimize the impact on service availability.

Geographic Redundancy

In addition to redundancy within data centers, we also employ geographic redundancy. This means having backup data centers in different geographic locations to ensure service continuity even in the face of regional disasters or outages.

Example: Our primary data center may be located in one region, while a secondary data center is located in a different geographical area, ensuring that if one region experiences a catastrophic event, services can be quickly restored from the secondary data center.

Load Balancing

Load balancing is an integral part of our redundancy and failover strategy. It ensures that incoming traffic is evenly distributed among redundant components, preventing overload on any single system and optimizing performance.

Example: When multiple users access our platform simultaneously, a load balancer distributes incoming requests to different servers, ensuring optimal response times and preventing server overload.

Real-Time Monitoring

Our systems are equipped with real-time monitoring tools that constantly assess the health and performance of critical components. This proactive monitoring allows us to identify issues before they escalate and take preventive measures.

Example: If the CPU usage on a server exceeds a predefined threshold, our monitoring system triggers alerts, and administrators can investigate and take action to prevent service degradation.

By meticulously implementing these redundancy and failover measures, Strike Labs not only ensures uninterrupted service but also aligns with the stringent standards set by CCPA, HIPAA, GLBA, COPPA, and the FTC. This unwavering commitment to system availability ensures that our clients can rely on our services even in the face of hardware failures, natural disasters, or unexpected disruptions, thereby maintaining data availability and business continuity in compliance with diverse regulatory frameworks.

Conclusion

At Strike Labs, we take immense pride in our ability to seamlessly integrate security and compliance into every product we create. Our core mission is not to be security and compliance consultants but to be architects of beautiful, secure software development solutions. We want you to know that when you choose Strike Labs, you're choosing a partner who prioritizes your data protection needs.

Our security best practices are more than just technical measures; they are a foundational element of everything we build. We understand that your operations rely on secure and compliant software, and we take this responsibility seriously. It's not about adding security as an afterthought; it's about ensuring that security is an integral part of the DNA of every product we deliver.

We also recognize the delicate balance between security and user experience. While security is paramount, we understand the importance of providing a seamless and enjoyable experience for your users. We don't just build secure solutions; we build solutions that are intuitive, efficient, and user-friendly.

Rest assured that when you choose Strike Labs, you're choosing a partner who is dedicated to safeguarding your network and data. We build with your mission and data protection needs in mind, ensuring that your operations remain shielded against potential threats.

If you're seeking software development solutions that are inherently secure and compliant, look no further. Contact us today to explore how we can assist you in achieving your security and compliance objectives. Your peace of mind is our promise, and your trust is our most valued asset.