www.dailystory.com | hello@dailystory.com

DailyStory Security Overview

Last updated August 4, 2018

About DailyStory

Since 2017, DailyStory has been on a mission to help our customers use digital marketing tools to grow their businesses by creating “Markets of One”. Our customers use DailyStory’s software, services, and support to transform the way they find new customers and keep them. DailyStory’s platform includes email marketing, text message marketing, social media publishing, blogging, CRM, landing pages, popups, reporting and analytics and more all in one integrated platform.

DailyStory’s products are offered as Software-as-a-Service (SaaS) solutions. These solutions are available to customers through purpose-built web applications, application programming interfaces (APIs), and open integrations.

Security & Risk Governance

DailyStory’s primary security focus is protecting and securing our customers’ and users’ data. This document outlines the security measures DailyStory have put in place.

Security & Risk Management Objectives

DailyStory's security framework is based on best-practices for software as a service businesses. This includes:

- ***Customer Data Protection*** – continually identify opportunities to enhance the security of our customers' most import asset: their data.
- ***Continuity of Service*** – ensure our customers' service is not disrupted by threats, such as denial of service attacks, or attacks on their APIs.
- ***Data Integrity*** – ensure that customer information is never corrupted or altered inappropriately. This includes auditing of customer actions as well as maintaining appropriate backups of their data.
- ***Standards Compliance*** – follow documented guidelines and standards both in the applications and in our data centers.

For additional information and common frequently asked questions about DailyStory terms of service, legal, and security, please visit https://www.dailystory.com/legal. There you will find links to other documentation, such as our terms of services, and security FAQs.

To ensure we protect the customer data, we have implemented the following security controls.

Product Infrastructure

Data Center Security

DailyStory hosts its products and services in the Microsoft Azure Cloud. Microsoft's Azure Cloud enables DailyStory's application to run in an enterprise-grade data center with multiple globally fault tolerant system redundancies. Additionally, Microsoft Azure provides DailyStory with industry standard data center best practices and certifications.

DailyStory does not host any production software systems within its corporate offices.

To learn more about Microsoft's Azure Cloud infrastructure, please see https://docs.microsoft.com/en-us/azure/security/azure-physical-security and https://www.microsoft.com/en-us/trustcenter/compliance/soc.

Network Security & Protection

DailyStory is designed and built with internet-scale security protections. Beyond the security features of the Microsoft Azure Cloud, DailyStory is designed with an overlapping set of security principles starting with the isolated nature of each instance.

The DailyStory application is composed of multiple distinct instances and each instance support one or more tenants. Each instance of DailyStory runs in one or more geographic locations and each instance is physically and logically separated from other instances.

Instances are segmented separately from one another and access to one instance does not grant access to another instance. Each instance can be further firewalled and isolated depending upon the needs of customers, such as blocking access to specific countries. This design provides a high degree of flexibility while maintaining security best practices per-instance.

This design further allows for DailyStory enterprise customers to run in isolated instances where no resources are shared with other tenants.

At the network level, databases and other data storage systems are further firewalled and restricted to exclusively allow access to the applications within the instance. Public access is controlled exclusively through the web application or the application APIs. No direct data access, such as for ETL or direct SQL is available to any customer. This ensures that direct customer data access is limited exclusively to the DailyStory application.

Changes in the network security model are actively monitored, and controlled by standard change control processes. All existing rules and changes are evaluated for security risk, and captured appropriately.

Configuration Management

DailyStory's infrastructure is managed through configuration profiles managed in Azure. This configuration management enables DailyStory to elastically scale based on customer demand both horizontally and vertically. Each instance of DailyStory follows a well-defined and established setup that is fully automated.

Configuration updates to a given instance are part of the application deployment automation and requires little-to-no human intervention. Changes to configuration management do not require access to the DailyStory application. Therefore, configuration changes do not require elevated permissions to access customer data.

Alerts & Monitoring

DailyStory's products are fully instrumented with alerting and monitoring 24x7x365 to notify our team when unexpected behavior occurs. Because of how DailyStory's instances are designed to run in Microsoft's Azure Cloud, customers may be running on different instances. Therefore, instances may be running different versions of the DailyStory application. And this allows DailyStory to roll-out or roll-back instances that exhibit problematic behavior.

All logins and other security related actions are logged. We additionally log failed authentication attempts. These logs are constantly monitored by our team and by our software to detect anomalies.

DailyStory Employee Access

DailyStory employees have limited access to customer data. When access to customer data is required for customer assistance or troubleshooting, that access is granted on an add needed basis. These types of requests are logged prior to permission grants.

Application Protection

Web Application Firewall

DailyStory relies upon application firewalls provided through the Microsoft Azure environment. DailyStory customers may additionally request for specific IP addresses to be blocked. DailyStory, at its discretion, may proactively block certain IP ranges or countries.

If you believe you are being blocked by a firewall restriction or would like a IP address or IP range blocked, please contact us.

Release Management

DailyStory's products are delivered on a continuous delivery approach with updates and improvements released daily or multiple times per-day. Code is reviewed, merged, moved into staging and then progressively rolled out to instances.

Automated testing and analysis is performed on all new code prior to being merged into a pre-production branch. Furthermore, new code requires additional unit and automation tests to ensure that new functionality behaves as expected prior to going into production.

Deployments to various environments (production and staging) can be instantly rolled back if problems occur. Various tenants run on different instances of the DailyStory software. This enables DailyStory to progressively roll out new features and capabilities. Major updates, improvements and bug fixes are documented in our product change log.

Vulnerability Scanning, Penetration Testing & Bug Bounties

DailyStory performs routine vulnerability scanning using industry-standard tools for a variety of potential attack vectors. This includes cross site scripting (XSS) for DailyStory's public JavaScript APIs and applications (forms, landing pages, etc.) and within the DailyStory customer portal.

Code analysis tools looks for potential vulnerabilities or patterns such that they can be detected early in the application development lifecycle. Additionally, DailyStory performs 3rd party security threat analysis and audits. This includes penetration testing. Penetration testing is performed against the application layer both in and outside of the portal as well as the public APIs.

DailyStory additionally offers bug bounties for defects identified by our customers. Please contact us for more information about bug bounties.

Customer Data

Managing Confidential Information

Data for our customers is collected from multiple sources included customer provided data sets, such as an import of contacts, as well as from public data sources. Per DailyStory's Terms of Service, DailyStory's portal and marketing tools capture customer data and store it on our behalf of our customers. However, it is our customers' responsibility to ensure they only capture appropriate information to support their marketing and sales processes. DailyStory is not able to discern the type of data that customers capture.

DailyStory products do not explicitly collect or capture financial information, such as credit cards, Social Security numbers, passport numbers, driver's license numbers or similar identifiers. While DailyStory does not explicitly capture this data, it is our customers' responsibility to ensure the data managed by DailyStory is appropriate for their needs and we have no direct knowledge of the type of data stored.

Credit Card Protection

Many DailyStory customers pay for the service by credit card. DailyStory does not store, process or collect credit card information submitted to us by customers. All credit card processing is managed by Stripe (https://stripe.com), a trusted 3rd party service.

Encryption In-Transit & At-Rest

Access to the DailyStory portal and DailyStory APIs require secure HTTP (TLS 1.2 and 2,048 bit keys or better) for encrypting data in transit.

Customers may host content with DailyStory on their own domain, such as landing pages and blogs. These do not require secure HTTP, but is recommended.

All sensitive data is further encrypted at rest. Specific fields such as login passwords, customer integration ids, oauth keys are further encrypted and/or hashed using industry standard best practices such as salting. Furthermore, all encryption and hashing uses salt unique to the user, tenant, and instance of DailyStory. This ensures that while two customers may choose the same password the values managed by DailyStory are unique.

User Authentication & Authorization

The DailyStory products enforce a uniform password policy. The password policy requires a minimum of 8 characters and a single special non-alphanumeric character such as: %, $, #. DailyStory customers may opt to utilize integrated sign in with Google, Facebook, and Twitter. By utilizing these services customers defer all password and identify management to these services.

Customers may use permissions through role based security within the portal to limit access to content and features available to other users of the portal.

DailyStory Application Programming Interface (API) access is enabled by granting API keys. One or more API keys are created from within the customer's portal. A key is used during the API request to grant privileges to use of the APIs. For more information please see DailyStory's SDKs and APIs.

DailyStory Employee Access

DailyStory employees may need access to customer data in production environments. This access may be because customer support is helping a customer troubleshoot an issue or when a software development bug is preventing a customer from accessing their portal.

All employee access to customer data is governed through role based security or just in time access. Just in time access requests are logged to determine which employees had access to which customer data sets.

Access to DailyStory infrastructure is limited through network access and user authentication and authorization rules.

Privacy

Your privacy is very important to us. Our privacy policy outlines our privacy approach in detail.

Data Retention Policy

Customer data is retained indefinitely in the DailyStory platform until it is requested to be removed. A request to remove data may be done through a GDPR data removal request or by submitting a request for data to be removed. Data is also removed if you are no longer a customer of DailyStory, however this can take up to 90 days.

Unlike data in production that can be deleted, customer data captured in backups, or other retention purposes, is naturally aged out as these backups are overwritten over time.

Privacy Protection Management

DailyStory works hard to ensure an effective and consistently implemented privacy program. Information about our commitment to the privacy of your data is described in greater detail in our Privacy Policy.

Business Continuity & Disaster Recovery

DailyStory's business continuity and disaster recovery plans focus on prevention and recover in the case of a disaster impacting us or our customers. This includes redundancy of system and business operations. DailyStory's goal is to isolate and address any issue and communicate with our customers transparently.

System Resiliency & Recovery

DailyStory's recovery and continuity process is validated continuously. The DailyStory application is constantly receiving updates on a continuous deployment process and creating new instances or tearing down instances is routine. DailyStory relies on infrastructure redundancy with multiple instances and redundancy of web applications, database and other components of the DailyStory application.

Additionally, DailyStory's application design enables portions of the application to be taken offline for maintenance with no impact to other running aspects of the application. This design further allows the DailyStory application to "recover" if certain aspects of the applications are experiencing problems.

Backup Strategy

Data, which DailyStory manages on behalf of its customers, is backed up and managed by Microsoft Azure. Backups are replicated across multiple Microsoft Azure data centers to provide fault tolerance and disaster recovery:

- Production data for our customers is fully backed up weekly, for up to 6 weeks, and point in time (snapshot) restorations for up to 10 days.
- Because DailyStory's applications are multi-tenant a database may contain information for multiple customers and DailyStory does not provide any hard copy backups for our customers.
- Backups and database snapshots are inaccessible to DailyStory employees and are fully managed by Microsoft Azure. DailyStory employees do not have access to customer data within a backup until a restore is created.

Incident Management

DailyStory monitors our infrastructure and applications 24x7x365. We respond immediately to any security and privacy events with a repeatable incident response playbook. All incidents are documented and once mitigated, a root cause analysis document is created and archived. When appropriate the root cause analysis document is made available to affected customers.

Our priority in incident management is determining the scope and source of the security problem. We then immediately communicate with any affected customers to coordinate resolution.

Product Security Features

DailyStory works hard to maintain the privacy of data you entrust with us. Data you store in DailyStory is yours. We put our security program in place to protect your data and use your data only to provide the DailyStory service to you. We never share your data across customers and never sell it.

Third Party Audits and Certifications

Our data center provider, Microsoft Azure, maintains ISO 27001, SOC 1, SOC 2, SOC3, and many other certifications.

Document Scope and Use

DailyStory values transparency in the ways we provide solutions to our customers. This document is designed with that transparency in mind. We are continuously improving the protections that have been implemented and, along those lines, the information and data in this document (including any related communications) are not intended to create a binding or contractual obligation between DailyStory and any parties, or to amend, alter or revise any existing agreements between the parties. For more information on DailyStory's legal policies, please see https://www.dailystory.com/legal/.