MyGet Security Policies

This document describes the MyGet security policies.

This enables you to be confident that your intellectual property and any personal or customer data will be well protected in our service in compliance with industry standards and regulatory requirements.

MyGet Security contact info: info@myget.org

Last modified on 2017-09-01.

INFORMATION SECURITY ORGANIZATION

High-level description of the service

MyGet is a hosted package repository service which stores and serves software components (packages) to consumers that have been granted access to the repository by the repository owner.

MyGet is a Software-as-a-Service product built on top of Microsoft Azure, our selected cloud service provider. As such, many security policies are already taken care of by Microsoft, e.g. facilities and physical data center security and contingency plans. More information can also be found on the Microsoft Trust Center web site: https://azure.microsoft.com/en-us/support/trust-center/.

Roles and responsibilities

MyGet's directors are responsible for applying Information Asset security (e.g. encryption of data at rest, access policies, transport level security). The principle of least-privilege is applied.

High-level description of the data-flow for the service

Payment and billing information is not handled directly by MyGet; instead, we leverage a third-party payment gateway (FastSpring) which ensures compliance with any applicable standards and policies.

Only the minimum amount of information required to identify a user is stored in our systems, such as a verified email address to create the MyGet user profile.

The package artifacts uploaded to and downloaded from our services are stored in Microsoft Azure storage accounts in either US or EU paired Azure regions. We typically choose the nearest location to you, but Enterprise customers can choose differently. For more info on paired Azure regions, see: https://azure.microsoft.com/en-us/documentation/articles/best-practices-availability-paired-regions/

Access is secured using industry-standard transport level security (HTTPS, SHA-2 certs, OAuth2 expiration/renewal tokens).

PII or other sensitive information

MyGet only collects the verified email addresses of users, the minimum required to be able to contact the user. More information about how we treat PII and sensitive information can be found in our Privacy Policy.

ASSURANCE CERTIFICATIONS; REGULATORY AND INDUSTRY STANDARDS

Industry standard certifications
Microsoft, our cloud service provider, has many industry standard certifications, which covers for the used infrastructure, storage and cloud services. More information can also be found on the Microsoft Trust Center web site: https://azure.microsoft.com/en-us/support/trust-center/. MyGet as a company, however, does not currently own any of these certifications.

Compliance with regulatory and/or industry standards

MyGet currently has no audit frequency schedule and does not provide copies of audit reports and certifications. On-site audits by customers or their representatives are not permitted.

EU PRIVACY SHIELD (EU SAFE HARBOR)	Compliant
EU GENERAL DATA PROTECTION REGULATION (EU GDPR)	Compliant
HIPAA	N/A
GLBA	N/A
SOX	N/A
PCI-DSS	Delegated to and covered by FastSpring, our selected reseller platform.

PERSONNEL SECURITY

Currently, no periodic background check processes are in place for personnel with admin access or access to customer data. Personnel must adhere to an acceptable use policy which is not yet formally documented.

OPERATIONAL SECURITY

We typically review our procedures twice a year, but update whenever we can improve.

Access Control Procedure
The principal of least-privilege is applied: access to customer data is only temporarily granted upon explicit customer approval using secured APIs.

Incident Management Procedure
MyGet has API monitoring and alerting on all services.

Change Control Procedure
N/A

Remote Access Policy

N/A

Document & Records Control Procedure

We use document versioning and keep track of document version history.

Backup Policy

All data is continuously backed up by our cloud provider (Microsoft). We take additional back-ups to cover for human-error (e.g. customer does accidental deletion of a package or feed, this would be auto-replicated to other regions, which is where our additional back-ups come in handy).

Vulnerability Management Policy

All devices connecting to our back-end services or storage are encrypted and have endpoint protection enabled.

Network/Host Security Procedures

(e.g. Hardening of Hosts, Firewall Approval Procedures, Anti-Virus maintenance procedure)
All devices connecting to our back-end services or storage are encrypted and have endpoint protection enabled.

Log Retention Policy

Currently, we retain all logs.

Disaster Recovery/Business Continuity Management Plan

MyGet services automatically failover within paired Azure regions. When required, we can additionally set up our services in other regions, but that requires a manual intervention.

Mobile/Personal Device Security Policy

All devices connecting to our back-end services or storage are encrypted and have endpoint protection enabled.

Third Party Outsourcing

Outsourced or Subcontracted (Parts of the) Services

Payments and subscriptions are handled by FastSpring, a third-party reseller platform. FastSpring handles payment and subscription data only, and takes care of all regulatory compliance and industry standards regarding payment processing and VAT.
Basically, FastSpring handles the payment aspect of our services, and only processes the minimum data required to be able to handle payments and subscriptions.

We regularly have our services scanned and audited for potential security vulnerabilities by Detectify.com, an external company specialized in security.

Use of Co-location (or similar facility)

MyGet does not utilize co-location or similar facilities. Any third-party who needs to connect to our systems is required to comply with our information security policies and procedures.

Network / Host Security and Vulnerability Management

The following policies are handled by and delegated to our cloud provider (Microsoft Azure):

- Systems involved in the service offering are protected by appropriate, industry-standard security controls (e.g. Firewall, IDS/IPS, Anti-Virus, HIPS, SIEM)
- Anti-virus signatures are updated in a timely manner when released by the vendor.
- A process is in place to scan, identify and remediate newly discovered security vulnerabilities on servers, applications and network devices.
- Patching, and frequency of patching, for servers, workstations, applications and network devices

The vulnerability and patch management process encompasses virtualization platforms. Anti-malware solutions are present at the Hypervisor level.

In addition, one of our customers has performed a penetration test for us to test our network security controls. No breaches were found. However, results are not shareable due to a confidentiality agreement with that customer.

On the application level, we use Federated Authentication as the authentication provider. Passwords are one-way encrypted.

Network / Host Security and Vulnerability Management

Compliance with Industry Security Standards
Our software applications, used for the service delivery, have been developed in compliance with OWASP, a known Industry security standard.

Security Penetration Testing
The application does not undergo 3rd party application penetration testing, however, upon customer demand, we may allow customer to perform such pen-testing against customer's own tenant.

Security Code Review
We don't use commercial Code Review tools (e.g. Fortify, Veracode) in the Software Development process. Our engineers received Application Security Training aimed at Developers (Microsoft SDL, see also https://www.microsoft.com/en-us/sdl/default.aspx).

IDENTIFICATION AND AUTHORIZATION

Access to Customer Data

No one in our organization has access to Customer Data, unless required to provide support to Customer, and after explicit approval has been granted by Customer, for this purpose only and limited in time. The principle of least-privilege is applied throughout.

We do not allow remote access to our systems, and we do never share Customer Data with third-parties or subcontractors.

Procedure to add, delete and modify user accounts and access

As an Enterprise tenant, Customer has an additional management dashboard where tenant administrators, appointed by Customer, can add, delete and modify accounts and access.

Security Auditing

Access to Customer data is logged and monitored for suspicious activity (such as unauthorized access attempts, security violations or authentication failures).

DATA SECURITY

Location of Customer Data

Enterprise Customers can choose geographical region where Customer data should be stored. MyGet currently offers Customer data to be stored in either EU or US data centers, but options may expand in the future.

Customer Data, including all of its copies and backups, are stored within the chosen Microsoft Azure regions.

Backup Policy for Customer Data

Periodic backup and recovery tests are handled by and delegated to our cloud provider (Microsoft Azure), which covers disaster recovery and technical problems on underlying service availability. MyGet takes additional weekly backups to cover for human mistakes.

Access to Customer Data Backups is restricted to the MyGet Support organization: the principle of least-privilege is applied throughout, and access is only granted temporarily when requested and approved by Customer beforehand.

Physical security controls to protect the backup data is handled by and delegated to our cloud provider (Microsoft Azure). For more detailed information, please refer to https://azure.microsoft.com/en-us/support/trust-center.

Data Transfer

MyGet only stores the data provided by Customer and required to deliver the service. Data will be transferred through a secure API over a secured connection.

Data Breach Remediation

As a EU-based company, MyGet is regulated by, and complies with, the EU General Data Protection Regulation (EU GDPR).

MyGet has not experienced any data breaches so far. In case of a data breach, we will assess the situation and reduce or even prevent access to the tenant-specific services, or if the situation requires block all access to our services.

Once our services are locked down to the extent needed to prevent further data breach, we immediately notify the impacted Customers and begin root cause analysis as well as investigation of what Customer data might have been affected by the data breach.

MyGet does not cover for all costs of remediation.

Customer Data Retention

MyGet retains Customer Data as long as configured by the Customer (e.g. through package retention policies or access token expiration settings).

Encryption

Data at Rest

Passwords and access tokens are always one-way encrypted (not recoverable).

All data that is written into Azure storage will be automatically encrypted by the Azure Storage service prior to persisting, and decrypted prior to retrieval. All data is encrypted using 256-bit AES encryption, also known as AES-256—one of the strongest block ciphers available.

Data in Transit

MyGet Services are only accessible over a secure HTTPS connection, ensuring data in transit is always encrypted.

AUTHENTICATION

Authentication Mechanism

A secure authentication mechanism has been implemented to access the service. By default, all services are only accessible over a secure HTTPS connection. Federated Authentication is configurable (e.g. Customer may decide which third-party Identity Providers are allowed, if any, or may choose to configure a corporate ADFS integration).

Internal MyGet staff uses the same authentication mechanism to access Customer Data through our services as Customers do (of course, only after permission has been granted by Customer, e.g. to handle a Customer Support request).

Authentications or logins expire after a period of inactivity.

Multi-factor authentication is currently not yet supported, but MyGet has it on the roadmap. When using a third-party Identity Provider (i.e. Google or Microsoft Account), multi-factor authentication is provided by the third-party Identity Provider.

User Account Provisioning

A mechanism is in place for provisioning or deprovisioning of internal user accounts in a timely manner. Tenant administrators appointed by the Customer can easily do this from the tenant administrative dashboard.

PHYSICAL AND ENVIRONMENTAL SECURITY

Physical and environmental security of Customer Data is handled by and delegated to our cloud provider (Microsoft Azure). For more detailed information, please refer to https://azure.microsoft.com/en-us/support/trust-center.
This includes:

- Customer Data resides in a physically restricted area
- Physical security controls to restrict and monitor access to the IT infrastructure involved in the service delivery
- Process for granting and revoking access to the restricted areas
- Physical access to the IT infrastructure involved in the service delivery, other than authorized IT personnel
- Reviewing of physical access rights on a periodic basis
- Restricting physical access to the service IT infrastructure (data center/server room) by using strong, multi-factor access controls, including biometrics
- Securing physical hardware used for service delivery
- Logging and auditing of physical access to the data centers hosting our services

MyGet does not permit transfer of Customer Data from its IT infrastructure to any external or removable storage media in any case.

PRIVACY

No formal Privacy Program, Privacy Awareness or Privacy Training program is in place.

However, MyGet does not collect any information for any purpose other than Customer's business purpose for which Customer uses our Services.

Upon termination of the service agreement between MyGet and Customer, or at the request of Customer, MyGet agrees to return all Customer Data, held or controlled by MyGet, to Customer, and will not keep any copies unless agreed otherwise in writing by Customer.

Unless prohibited by law, MyGet will promptly notify Customer if a request to access Customer Data has been made.

AVAILABILITY AND BUSINESS CONTINUITY MANAGEMENT

Most of MyGet's Availability and Business Continuity Management is delegated to and handled by our cloud provider (Microsoft Azure). More information about Microsoft Azure Data Centers can be found at https://www.microsoft.com/en-us/cloud-platform/global-datacenters.

This includes:

- Conducting regular risk assessments for processes included in the Disaster Recovery/Business Continuity Management plan
- Data replication over multiple data centers used to reduce the impact of a disaster
- Conducting regular tests to ensure failover capabilities are in place and operating as expected
- Ensuring optimal distance between data centers (see also https://azure.microsoft.com/en-us/regions/)
- Ensuring data centers are located in different power grids
- Using redundant components in our servers (such as power supplies and NICs)
- Providing power backup in case of a power outage
- Monitoring servers for components failures
- Clustering or load balancing to prevent service disruption due to infrastructure failures
- Using array-based replication where applicable

TENANT SEGREGATION

Customer Data Segregation
MyGet Enterprise tenants use dedicated storage accounts to handle Customer Data. This means data is stored in separate Microsoft Azure Storage Accounts which are secured using their own separate access tokens.

In case of a legally required extraction of Customer Data, targeting another Customer, there is no impact on other Customers or other Customer Data.

Customer Data Traffic Segregation
Customer Data served directly from the Customer's dedicated Microsoft Azure Storage Account is not shared with anyone else.

For the NuGet protocol, there is a distinction to be made between the v2 and v3 NuGet protocols.

- The v2 NuGet protocol traffic is shared by VM's that perform the protocol translation.
- The v3 NuGet protocol segregation is performed at the storage level, in this case traffic is isolated.

INTEGRATION

Email Integration
The MyGet service offering does not currently include the sending of email communications on behalf of Customer. Emails sent from the MyGet Services will typically use noreply@myget.org as the "Envelope Sender", "From" and "Reply-To" addresses.

Certificates
MyGet is not required to store any Customer Certificates on its servers as part of the service offering.

SAML-based Federated Authentication
MyGet supports SAML-based Federated Authentication. An API for provisioning is not yet publicly documented but can be made available upon request.

Data Exchange over SFTP
MyGet does not offer an SFTP service for data exchange.

Customer Domain Names
MyGet Enterprise Customers can choose their preferred subdomain to MyGet.org, i.e. customercompanyname.myget.org. Customer can register CNAME records for its own domain names in DNS pointing at this myget.org subdomain, however, we generally recommend not to do so.