April 2019

PackCity

FAQ - IT Security

Where do you store customer's data? (Geographical localization)

Our PackCity Solution is hosted at Interxion datacenter located in Europe (France - Marseille). This datacenter is certified ISO 27001 and ISO 22301.

Does your organization have appropriate physical access controls in place to ensure only authorized staff have access to relevant systems?

Physical data center access is only restricted to authorized employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

All equipment is checked upon arrival. Visitors are screened upon entry to verify their identity, and in shared situations, are escorted to their appropriate locations.

We also restrict personnel access to all hypervisor management functions or administrative consoles on the principle of the least privilege.

Please provide an overview of your system / application architecture

Each exposed component is hosted in its own DMZ. Explicit firewall rules between DMZ are applied to allow known traffic only. Access to database server is limited to requests only from these DMZs.

The servers and web site are based on LAMP (Linux / Apache / MySQL / PHP) servers.

What type of hardware, operating systems and user interface environment are supported on the desktop PCs or workstations?

Packcity Web tracking application (NISS) requires a PC with the following minimum features:

- Windows 7, Windows 8, Windows 8.1 or Windows 10
- 2 Ghz CPU, 32 or 64 bits
- 1 Gb RAM
- 50Mb free hard-disk space

The Web application requires a web browser such as Google Chrome, Mozilla Firefox or Microsoft Edge. It is recommended that you update your browser with the latest version to support the latest security fixes, performance improvements and internet standards. Microsoft Internet Explorer and Apple Safari are not supported

As the application can export report in PDF, a PDF reader application needs to be installed to correctly view these reports.

How is security handled by the application? E.g. authentication method, password controls, user access?

Our applications can only be accessed by registered users and their view depends on their privileges. Authentication is done with a user login and password.

If the application is web-based, does it support SSL/HTTPS? If yes, what encryption is supported?

Our web application has a standard RSA 2048 bit certificate to protect data in transit and used the TLS 1.2 protocol.

Does your platform have security protection against the OWASP Top Ten Web Application Vulnerabilities? This includes input validation, output escaping and SQL injection protection (e.g. parameterized queries)?

There are procedures in place to triage and to remedy reported bugs and security vulnerabilities for product and service offerings. We have the capability to rapidly patch vulnerabilities across all of our computing devices, applications and systems. Additionally, source code analyzers (like Checkmarx or Burp) are also used to avoid OWASP vulnerabilities.

What measures do you have in place to provide assurance of the security of your products? E.g. application penetration test results, SSAE16 etc.?

Vulnerability checks are performed weekly and manage accordingly to the Vulnerability & Patch management. Intrusion and security testing is conducted on software application periodically and prior to any software release.

Do you perform application penetration testing and vulnerability scanning? If not, do you permit external security tests to be conducted on behalf of your clients? Do you share the results?

Yes, at least once a year or on customer request (at customer expense). Results are analyzed, and Patch management is applied to correct issues if discovered.

Do you have security incident response procedures in place to manage occurrences of incidents such as Denial of Service, website defacement, data breach and phishing?

We review applications for security vulnerabilities and address any issues prior to deployment to production.

Once an issue is identified, our process is to place issues into our current sprint for development. Once item has been developed it will be subject to peer code review and then will be passed to QA department that will review and test items. A hot-patch is generated for the solution in to our production environment for urgent patches.

Do you have malicious code protection (e.g. anti-virus, Intrusion detection systems)?

An HIDS (Host-based Intrusion Detection System) (OSSEC) is used to protect the Packcity server against installation of unauthorized software. On Neopost workstation and Windows servers, Kaspersky antivirus is also used to scan the application against virus or malicious Software. Antivirus is automatically updated.

Can you provide historical data concerning availability?

Packcity committed uptime availability is 99,5%, on a yearly basis, excluding routine maintenance and downtime from interruption, termination, or failed operation of the Internet, private intranet, or of third-party telecommunication services and force majeure events.

What is your downtime plan (eg, service upgrade, patch, etc.)?

One week-end per quarter is reserved for service upgrade if necessary. Most of operations are done out of business hours.

How is client data protected?

Client data is stored in a secured sub network (MZ), which is not accessible from WAN, but only from web servers (DMZ).
Direct access to database is restricted and can be done only by authorized staff.
Neopost guarantees and commits that customer data are not used for any business or any Marketing purposes.

How do you separate my customer data from other customers' data?

Customers' data are stored in in a multi-tenant database databases and are not encrypted.
Access policy for the customer is set on application level.

How is user access managed within your solution?

User can access only with their login and password. All requirements and trust levels for customers' access have been defined and documented.

What is end-user password policy?

Manage through Active Directory policy application. Strong password with at least 8 character with 1 upper, 1 lower, 1 number, 1 non-alpha. Renewal all 90 days. Keepass tool is used to store in a secure way passwords.

What mechanisms are in place for clients to enter data in PackCity Cloud?

Data entry is performed manually through the application web site. Also, email addresses and contacts can be imported manually or automatically via FTP, FTPS and SFTP.

What is your data backup, recovery?

The application server and database are backed up nightly to an external site. Backups are not encrypted.
RTO (Recovery Time Objective) = 4 hours.
RPO (Recovery Point Objective) = 24 hours.

What is the process for prioritizing and resolving incidents relating to the system?

For PackCity locker system, SLA is the following:

Priority level	Issue level	Resolution Target Datacenter	Resolution Target Software
Priority 1 – P1	**Critical**	90% <= 3 hours	90% <= 3 hours
A service, system, network and/or a piece of configuration identified as Business Critical is totally down. The issue shows on or more of following points: • No functionality is accessible • File exchange (EDI) on critical flow is not possible • A majority of users on one or more sites are impacted • No issue bypass available/possible. • Disaster in progress with a critical business impact			
Priority 2 – P2	**Major**	90% <= 8 hours	90% <= 1 day
This applies when a service, system, network, software or piece of configuration can be used but with low performance and/or with very limited functionalities. Customer operation can continue in degraded mode. The issue shows one or more of following points: • Related to a critical service, network, software or piece of configuration but in a less urgent context than in Priority 1 • Some functionalities are unavailable, the system can be operated in degraded mode, but a solution must be provided quickly • The issue or slowness appears in a period considered as Critical			
Priority 3 – P3	**Minor**	90% <= 3 days	90% <= 15 days
This applies to issues with limited effect on customer operation or software availability, meaning that the application is lightly degraded. Hereunder a list of possible minor issues: • Issue where a customer acceptable bypass is available • Slowness of the File exchange service (EDI) on non-critical data flows			
Priority 4 – P4	**To Be Scheduled**	Next release	Next release
This applies to issues having no effect on customer operation. Hereunder a list of possible P4 issues: • Issues on user interface having no impact on functionalities			

What is the data retention policy (mainly package tracking data)?

By default, data retention time is 12 rolling months. After this period, data are deleted in the database. All data are deleted at the end of the Customer's contract.

Do you have a rigorous testing and acceptance procedure for outsourced and packaged application code?

Each version is subject to code peer-reviews to detect security vulnerabilities and address any issues. We have controls in place to ensure that standards of quality are being met for all software development. Each version will be tested by our Software Quality Control team prior to deployment to production.

Are third parties involved?

Yes. The Packcity Datacenter and the Neopost subsidiaries. Penetration tests include these third parties.

What about third party apps (components) that you use in your services?

We only engage with 3rd parties and subcontractors who are compliant with necessary security and privacy laws. Each version is tested by our Software Quality Control team prior to deployment to production.

Will any third party, including government agencies, have access to my customers' data? If yes, under what conditions?

No, except if requested by law.

What data do you collect about my staff or other people related to my business operations (logs, etc.)? If data is collected, describe how and for how long it will be stored?

As the application gives the ability to manage Parcels Locker machines and track parcels, we collect user, recipient, mail/parcel attributes information. These pieces of information can be used for support purposes such as bug fixing but are never used for any commercial purposes (marketing, stats, …).

Are there shared logs accessed by third parties with risk of revealing information about my staff and other related people?

No. Access to logs is strictly restricted to authorized staff. Log files are not shared with third parties. We keep only information about modification that each user has performed on the status of a package or any modification on the parcel Locker.