DEVOLUTIONS COMMITMENT TO SECURITY

Table of contents

1. Introduction

Devolutions Inc. is committed to provide the safest products and due diligence care in handling customer information. We employ industry-leading frameworks, standards and best practices to implement strong processes and controls. This commitment led to the implementation of various security measures aimed at preventing and mitigating threats that may have a potential impact on our customers' data or ability to provide our services.

2. Reporting a Security Issue

While we do take care of the security of our products, the fast-changing nature and complexity of security may expose inadvertently our software or supporting infrastructure to vulnerabilities. If you identify such vulnerability, please send us your report in a timely manner at security@devolutions.net. The report should include the following items;

- Proof-of-concept code and relevant screenshots to help us confirm and reproduce findings.
- Justification of how the impacts may affect our organization and/or customers if exploited.
- Proposed fix, if possible and applicable.

Once submitted, allow us a reasonable time to provide some feedback. Our security team must;

- Reproduce and confirm the vulnerability as described in your report.
- Establish a severity score according to CVSS 3.0[1].
- Consider the recommendations from your report and build an action plan with relevant teams.
- Maintain communication with the reporter until the case is resolved.

Due to the sensitive nature of a security report, we highly recommend encrypting your report using our **GPG public key below**. GnuPG software for Windows is free and can be downloaded at the following address: https://www.gpg4win.org/


```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBFywmrIBCAC8+MTiQLl7rZySJVO/w71Bhe+ej6od7DxB4/mkNcfKr83YRlYX
OBMyE8kavsdk++7H6QuEZIKibHxytJFPhVmsGJxh8VPbLcOvcCQyrv6gGRykf3lx
MQzbpsKtd+N9dSHd9I5epsMO4n69O6h6uIvU9yGDKOeUNp/RWHNpT4vL3c+UULq2
z/C6a+uVKxf91BbsmIawh1WrgpaSDjUO1r8W/Z2OJMHsfu/qv47oUMK+j3Ka4bW3
PFWGp8o94z7EsP9J9ZfiWZ/dwRGYsETO38D7lPfMocnDb/cowyUQsyCRCoPbnOqv
d2rUvGC7xtx1F++YKQ6QeL9sQL2jUhC5oZYNABEBAAG0I1NlY3VyaXR5IDxzZWN1
cmlOeUBkZXZvbHVOaW9ucy5uZXQ+iQFUBBMBCAA+FiEEM+2hCHRM3hIKDgBissc/
+n/SykMFAlywmrICGwMFCQlov84FCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQ
```


[1] https://www.first.org/cvss/cvss-v3-guide.pdf

ssc/+n/SykOq8Qf8CMyKzbO7PmqkGclRjirL/N9Ulqt1WSkMuB65G4fSbVnJeumG
Z5IhKT62kLtpOcOM4a6mBaHh3rq6jSJ1xEBMrFbKx6k53dDMbmFMlk8IDrDSSnI4
DzFFVJ78c4PSLaWJlvFnBOGlvDu8YQJLeCFjEr7OKwENw8cmzFcOcLupXvS3Gjry
fkIsphj4501fJF7TC5EuTHu1XGZxYRHB9ze+82bJFtyrXuKkkuAOTFfkOwF+wk3j
EPWOz29iZvYlkzK9v4fkVWXTQWAgGXqCjLLTaFhb3pFD8wuu/Q4ag+M8HmBcO3ll
TIz3xmmDwcZo/RZ8TNmneZ2NUshHN2s+9mZOn7kBDQRcsJqyAQgAscsxQKW8XtS8
J7aDTdwkb59dTyeJ7GOGMFDYrQpswsNwHNtZpgrRpVVNoF2GDi8Idpqhb7ShfOS8
3p5hLUvFO1G5i1/gwfKJjldBPBW4T7SpJ582FFK1KeT7x8WKlKmfNr9RX8s79dCp
6Kv38Lj5Lv6fh69yXCT1gMOPmjbL8XuvaY6QqzHCODAHJpEcXzXzDINsU3/BVIfK
p3i4dw7GzuXco2dbP5DGQjwCg+Dy1TzOzlV+uCOU+f33Agt+3I7s+e7ATPIMxnAX
KKUgQZS/2kpj1PWsEJPR4FjOLcYu9QRJ7UgFB4/OAWRkl54jl+78BPSTS7uCLe3c
mDauaSh6QwARAQABiQE8BBgBCAAmFiEEM+2hCHRM3hIKDgBissc/+n/SykMFAlyw
mrICGwwFCQlov84ACgkQssc/+n/SykNHqAgAgXO1mI95mMhkEgjqJRv3eqjqOR6S
fwL6rlw2lIrYHiFlVqXNZngJw7CrHGFAsJOOMAaqMXaRqXL2LiU6922JYlMum2AG
FDQ3yzxojbWZpylw3iTvQGwDElKfV8Y/d1Kxic5UfUC/VQdWgGM4iqgeoc7GPhMu
n+duvS48tnuqFKxYgr/hF/WWUmrfkbWJmZAHNrhaGBfU4i7N1iWYVjDinkPE6RZw
oaibhLsodaU5AltHSW/VjehiOu63CPrl6hjt/aD5GEpolqhGG9Mpc7xrOcFTDHAB
N8MA+E7AmEyz1g2vO2uskwOOKzWBroXDID1d1vkOxbSm2LS5BOVfFcGuGQ==
=KH/J
-----END PGP PUBLIC KEY BLOCK-----

We kindly ask to maintain the report and its content confidential until the appropriate corrective measures are released in production. Also**, exploiting a reported vulnerability abusively or for illegal, malicious or other inappropriate purposes may result** in legal prosecutions against the reporter which could lead to civil or criminal liability. An action is considered abusive or inappropriate when used for any purposes other than for the demonstration of a vulnerability, or when such action compromises customer-related or internal confidential information in an undue or disproportionate manner**.**

3. Enterprise Risk Management

Our risk management framework is based on industry standards and is deeply integrated into our business structure from governance to daily operations. This approach allows us to strengthen our commitment to security by allowing the right enablers to identify, assess, respond and monitor our risks. It is a vital topic of our Information Security Policy and our staff is trained to maintain a risk-aware culture to foster a healthy, reliable and secure environment for our business and our customers.

4. Reliability

The era of cloud solutions is inevitable when it comes to reliability. Our infrastructure, supported by Microsoft Azure Cloud, offers availability and redundancy to our online services and operations. System failures and downtime are greatly minimized by this technology.

Backup operations, business continuity and disaster recovery strategies are planned, implemented and tested to ensure resiliency against unforeseeable events.

5. Data Protection

Data at rest and in transit are exposed to many threats. We use strong tactics, technologies and procedures to safeguard customer data against confidentiality and privacy breaches. More specifically;

- Sensitive data at rest is encrypted using strong AES-256.
- Encryption keys are secured using dedicated technologies including KMS and KDFs.
- A formal vulnerability management policy assures identification and remediation of weaknesses and vulnerabilities before they can be exploited.
- Penetration testing and code review activities are performed regularly to minimize the presence of exploitable vulnerabilities on our production infrastructure and in our products and services.

The above list is not intended to be exhaustive and additional controls may be implemented from time to time.

6. Data Access

Access to our production infrastructure and data is limited to authorized personnel only. Strong authentication schemes with Multi-Factor Authentication (MFA) are enforced over encrypted channels to identify our personnel.

Role-based access controls and component isolation limit access to “who needs to know” in order to enforce the “least privilege” security principle and strategy.

Physical access to our data centres is secured by the controls enforced by Microsoft Azure Cloud security measures. The effectiveness of their controls is documented by external auditors and are reviewed annually by our security team.

Logging and monitoring systems are in place to audit for unauthorized access attempts and suspicious activity. A periodic review of privileged access rights is also performed on our production systems.

7. Secure Operations

Our hiring process requires every new employee to be screened for criminal records. We push even further by screening employees with privileged access authorizations every two years.

Our change control policy and processes assure that new code and systems are developed and tested in a dedicated staging environment before being approved and deployed in production. Maintenance windows are communicated to customers.

A formal security awareness program that measures and improves security awareness of individuals within the organization. Specialized security training from industry-leading firms are sponsored annually to improve knowledge and skills related to security for relevant personnel.

8. Incident Response

Our incident response plan is tested periodically to assure identification, detection, analysis, containment, eradication and recovery of security events. Security events reported to the Incident Response Team (IRT) are triaged and escalated according to the severity of impacts. Third parties may be involved in the resolution of an incident such as law enforcement, service providers and external firms. A communication plan is in place to protect confidentiality and privacy of customer information during treatment of a case.

The organization consumes and collaborates with various threat intelligence sources to optimize detection and response performance as well as identifying new emerging threats.

IRT personnel is trained on a regular basis by taking industry-leading security training and certifications. IRT is tested against simulations periodically to evaluate and improve overall team performance.

9. Compliance and Audit

The organization fulfils its obligations towards regulatory and compliancy requirements annually. More specifically, Devolutions maintain;

- PCI DSS compliancy by transferring all its payment operations to a certified level 1 payment partner; Stripe. No payments are processed, transmitted or stored by any Devolution-owned system.
- Privacy of its customer data by implementing technical, physical and organizational measures and safeguards which comply with applicable data privacy laws and regulations such as PIPEDA and GDPR.

Work with external auditors has been initiated on an annual basis to provide an independent opinion on the effectiveness of our security measures. Any gap identified is remediated within a reasonable timeframe.

10. Shared Responsibility

Security is everyone's responsibility. The customer plays a key role in maintaining confidentiality and privacy of its own data. More specifically;

- The customer has the responsibility to update and upgrade its software to the greatest version to maintain the optimal level of security.
- The customer must configure its software according to the security guidelines published on our own web site.
- The customer should promptly contact support for any security-related questions on deployment, configuration and best practices about the product or service usage.
- The customer must promptly report any security-related bug or vulnerability as elaborated at *Section 2 Reporting a security issue.*