Penetration Testing Process

**Penetration Testing – Microsoft Azure operated by 21Vianet**

Microsoft Azure operated by 21Vianet takes the security of our platform very seriously, and we have implemented a number of [technical and procedural measures](https://www.trustcenter.cn/en-us/) to help with platform security. These include identity and access management, mutual SSL authentication, layered environment, monitoring, logging and reporting.

We understand that security assessment and testing is an important part of our customers’ application development and deployment. We have established a policy for customers to carry out authorized penetration testing on their applications hosted in Microsoft Azure operated by 21Vianet. *Because such testing can be indistinguishable from a real attack, it is critical that customers conduct penetration testing only after notifying and obtaining approval in advance from the Microsoft Azure team and only in accordance with our terms and conditions.*

If your penetration test process meets one of the following conditions, you do not need to apply for penetration test authorization. We allow you to perform penetration test, but you still need to comply with the terms and conditions of penetration test in this document:

1. The test destination address is the customer’s Azure private address;

2. The test destination address is the customer’s Azure public address, the test source address is the customer’s Azure public/private address, and both the source and destination address belong to the **SAME** customer.

**In addition to the above scenarios, you will need to apply for penetration testing approval.**

**Penetration Test Approval Process:**

1. *Initiate Approval for Penetration Testing*

To obtain approval for penetration testing, please complete the ‘Penetration Testing Approval Form’, and then contact us via hotline(400 0890 365) or <https://www.azure.cn/support/contact/>. After successful submission, you will be provided with a reference number, which can be used for any further communication related to this request.

1. *Approval from Microsoft Azure Team*

Once the form is submitted, the Microsoft Azure team will respond to the request within five business days. In case any further information is required, the Microsoft Azure team will contact you by email using the information provided in the ‘Penetration Test Approval Form’. You can track the status of the request using the reference number provided during submission of the request.

1. *Test Completion*

You may only conduct those tests approved by the Microsoft Azure team and subject to any conditions specified in the approval email. In case you require additional time (or a different time) to carry out the testing, you must submit a new request for approval. The testing can only be carried out after authorization by the Microsoft Azure team for the new dates.

If you believe you have discovered a potential security flaw related to Microsoft Azure operated by 21Vianet or have other questions about penetration testing or the status of your request, you can reach us at<https://www.azure.cn/zh-cn/support/contact/>.

Penetration Testing Approval Form

|  |  |
| --- | --- |
| **Name (Primary contact point)** |  |
| **Email address** |  |
| **Phone number** |  |
| **Microsoft Azure subscription ID** |  |

1. What is the purpose of your test?
2. Who is carrying out the penetration test (Internal Team or Third Party)?
3. If penetration test is going to be conducted by Third Party, please provide the following details:
   1. Name of third party
   2. Contact person
   3. Email address
   4. Phone Number
4. If you want to apply for penetration testing exercise, you must finish the form as below :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Brief description of test | Target DNS names for testing (\*.chinacloudapp.cn) or test destination IP address | From where will the test be launched?  (IP address of hosts) | If applicable, name of open source/ commercial tool that will be used | Test start date and time with time zone (+/- GMT) | Test End date and  time with time zone (+/- GMT) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. Additional comments

**Penetration Testing Terms & Conditions**

By submitting this form, you agree that the information you have provided is true and accurate and to the following terms and conditions:

1. You are the owner of the Microsoft Azure subscription specified above and authorized to conduct penetration testing against that subscription.
2. Your testing will not target any other subscription or any other customer of Microsoft Azure.
3. You will not conduct any Prohibited Tests or Test Behavior (see below).
4. You will not conduct any tests that will exceed the bandwidth quota for your subscription (ask Customer Support if you are unsure).
5. You will conduct only those tests approved in the authorization email from the Microsoft Azure team for the time and duration the Microsoft Azure team specifies.  You will abide by any other restrictions or conditions the Microsoft Azure team specifies in the authorization email or any subsequent communication from the Microsoft Azure team regarding these tests.
6. Your testing will be in accordance with the information you provide in this form, except where the Microsoft Azure team specifies otherwise.
7. If during the course of your testing, you believe you have discovered a potential security flaw related to Microsoft Azure, you will report it to the Microsoft Azure team at <https://www.azure.cn/zh-cn/support/contact/>within 24 hours and will not disclose this information publicly or to any third party for at least 90 days.
8. Your use of Microsoft Azure, including this testing, will continue to be subject to the [terms and conditions](https://www.azure.cn/support/legal-en/) of the agreement(s) under which you purchased Microsoft Azure.
9. You are responsible for any damage to Microsoft Azure or other Microsoft Azure customers that are caused by failure to abide by this agreement.

**Prohibited Tests or Test Behavior**

1. Performing any kind of denial of service testing, or any other test designed to determine, demonstrate, or simulate any type of denial of service.
2. Performing automated testing of services that generates significant amounts of traffic.
3. Scanning or testing assets belonging to any other Microsoft Cloud customers.
4. Gaining access to any data that is not wholly your own.
5. Performing network intensive fuzzing against any asset except your Azure Virtual Machine
6. Deliberately accessing any other customer’s data.
7. Moving beyond “proof of concept” repro steps for infrastructure execution issues.
8. Attempting phishing or other social engineering attacks against our employees.

**Privacy**

The information you share with us in this form will be kept confidential and used only to assist us with respect to your penetration testing or improving the security of Microsoft Azure.  Please see our [Privacy Statement](https://www.21vbluecloud.com/dynamics365/d365-privacy/) for more details.