

# Annex I: VAPT – Scoping Document

Government of Nepal

नेपाल सरकार

Office of the Prime Minister and Council of Ministers

प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय

National Cyber Security Center, Singhadurbar, Kathmandu

राष्ट्रिय साइबर सुरक्षा केन्द्र, सिंहदरवार काठमाडौं

VAPT Request Form

जोखिम पहिचान तथा सुरक्षा परीक्षण (भि.ए.पी.टी.) अनुरोध फाराम

## 1. Organization Details (कार्यालय विवरण):

Organization Name (संस्थाको नाम): \_\_\_\_\_

Contact Person Name (सम्पर्क व्यक्तिको नाम): \_\_\_\_\_

Email (ई-मेल): \_\_\_\_\_ Website Name (वेबसाइट): \_\_\_\_\_

Mobile Number (मोबाइल नं): \_\_\_\_\_ Telephone Number (टेलिफोन नं): \_\_\_\_\_

Address (ठेगाना): \_\_\_\_\_

PIS/EmpidId (संकेत नं/कर्मचारी नं): \_\_\_\_\_

# Annex I: VAPT – Scoping Document

## 2. Testable Environment Details:

1. **Application/Website to be tested:** The testable URL/domain, subdomain and IP addresses used for the application/website to be Vulnerability Identification and Security Testing (VAPT) must be a replica of real system hosted under the Integrated Data Management Center (IDMC) (.gov.np or .org.np). **Note:** In addition to real systems hosted in IDMC, test instances hosted on external hosting for testing purposes are also allowed to be used for security testing.

(जोखिम पहिचान तथा सुरक्षा परीक्षण (भि.ए.पी.टी.) गर्नुपर्ने एप्लिकेशन/वेबसाइट: जोखिम पहिचान तथा सुरक्षा परीक्षण (VAPT) गर्नुपर्ने एप्लिकेशन/वेबसाइटहरूका लागि प्रयोग गरिने यूआरएल/डोमेन, सबडोमेन तथा आईपी ठेगानाहरू एकीकृत डेटा व्यवस्थापन केन्द्र (IDMC) अन्तर्गत (. gov.np वा .org.np) मा होस्ट गरिएको वास्तविक प्रणालीको रेप्लिका हुनुपर्नेछ। नोट: IDMC मा होस्ट गरिएका, परीक्षण प्रयोजनका लागि बाह्य होस्टिङ मा राखिएका परीक्षण प्रति हरेलाई पनि सुरक्षा परीक्षण गर्न अनुमति प्रदान गरिएको छ।

2. Does the application include any custom workflow or button process that should be included (Example: Application/Registration process, document verification, renewal process etc.)?

२. के आवेदनमा समावेश गर्नुपर्ने कुनै अनुकूलित कार्यप्रवाह वा बटन प्रक्रिया समावेश छ (उदाहरणका लागि आवेदन/दर्ता प्रक्रिया, कागजात प्रमाणीकरण, नवीकरण प्रक्रिया आदि)?

Yes

No

Not Sure

If yes please briefly describe or share supporting documents, including user manuals, technical documentation, and, where available, video tutorials. If possible, provide hands-on support during system setup, either physically or virtually.

## Annex I: VAPT – Scoping Document

3. Please list out the path of URLs or buttons (Logout, Delete, Update/modify, administrative or privileged actions, Payment, transaction, or financial processing functions etc. or Any API endpoints or backend functions) that should not be clicked/restricted (Example: /logout, /delete-user, /admin/delete/\*,, /update-profile, /modify-record,/transaction/process etc).

३. कृपया क्लिक गर्न नहुने यूआरएल अथवा संवेदनशील बटनहरू (लगवाउट, डिलिट, अपडेट/ मोडिफाइ आदी), प्रणालीका कार्यहरूको सूची उल्लेख गर्नुहोस् (उदाहरण: /logout, /delete-user, /admin/delete/\*,, /update-profile, /modify-record,/transaction/process आदि)।

4. Please provide a list of URLs, endpoints, or application paths that are not directly accessible or visible through the public website interface, but exist within the system (Administrative portals, Backend or management interfaces, Hidden APIs or service endpoints not exposed in the UI, Testing, staging, or debug paths, Direct-access URLs that require manual entry or prior knowledge).(Example: /admi portal,/backend/login,/internal/api/v1,/test/environment, /hidden/dashboard)

४. कृपया URL हरू उल्लेख गर्नुहोस् जुन प्रत्यक्ष रूपमा उपलब्ध छैन वा वेबसाइटमा लुकेको छ (उदाहरण: /admi portal,/backend/login,/internal/api/v1,/test/environment,/hidden/dashboard))

# Annex I: VAPT – Scoping Document

## 3. Basic Detail (आधारभूत विवरण):

1. What is the website development platform? १. वेबसाईट विकासको प्लेटफर्म कुन हो?	
1.1 Frontend with Version	
1.2 Backend with Version	
2. Which database used? Mention the database version. २. प्रणाली/एप्लिकेशनमा कुन डाटाबेसको प्रयोग गरिएको छ? डाटाबेस संस्करण उल्लेख गर्नुहोस्	
3. Is payment gateway integrated with the application? If yes, how many? ३. प्रणाली/एप्लिकेशनमा भुक्तानी गेटवे एकीकृत रहेको वा नरहेको ? रहेको भए कति वटा रहेको?	
3.1 Details with Version	
4. How many authorization levels are there? ४ प्रणाली/एप्लिकेशनमा आधिकारिक तह कति रहेका छन्?	
5. Do you want Credential based or Non-Credential Based Scanning? ५ प्रणाली/एप्लिकेशन प्रमाणमा आधारित वा प्रमाण रहित, कुन स्क्यान गर्ने ? If Yes, Please provide the details for every user role , credential and required level (Normal, Reviewer, Approval, Admin, SuperAdmin etc.)	

## Annex I: VAPT – Scoping Document

6. Is there additional set of access credentials? ६. पहुँचका प्रमाणहरू सेट गरिएका छन् ?	
6.1 Encryption Standards (SSL /TLS versions, key lengths, and data-at-rest encryption)	
6.2 MFA/SSO Config (Multi-factor authentication, SSO, or temporary bypass setup)	
6.3 Digital Signature or Client Certificate	
7. Do you want to utilize sensor-based scanning in VAPT? ७. के तपाईं VAPT मा सेन्सर-आधारित स्क्यानइड प्रयोग गर्न चाहनुहुन्छ ?	
<input type="checkbox"/> Yes	
<div style="border: 1px solid black; padding: 5px;"><input type="checkbox"/> JAVA <input type="checkbox"/> PHP <input type="checkbox"/> .NET <input type="checkbox"/> Node.js</div>	
<input type="checkbox"/> No	
8. Tools used for audit (VAPT) if any ८. जोखिम पहिचान तथा सुरक्षा परीक्षण (भि.ए.पी.टी.) लागि कुनै औजार/उपकरणहरूको प्रयोग गरेको भए उल्लेख गर्नुहोस ।	

# Annex I: VAPT – Scoping Document

## 4. Additional Details:

Name	Number
Server Details	
Application Server	
Database Server	
Load Balancer	
Third-party Service integrations (API Gateway / Host/Version/URL/ Authentication Type/ Testing Permission/Documentation)	
Number and Location of Application Backup	
Number and Location of Database Backup	

I/We hereby agree to allow NCSC to conduct Vulnerability Assessment and Penetration Testing (VAPT) test on the above-mentioned address/links. Further, I/we declare that

(म/हामी माथि उल्लिखित ठेगाना/आईपीमा राष्ट्रिय साइबर सुरक्षा केन्द्र बाट गरिने जोखिम पहिचान तथा सुरक्षा परीक्षण (भि.ए.पी.टी.) गर्न मञ्जुर छु/छौं । थप म/हामी यो घोषणा गर्छौं।)

The above-mentioned address/link should host on Integrated Data Management Center (IDMC) and contains exact replica of the system to be tested.

(माथि उल्लिखित परीक्षण सर्भरको यू.आर.एल. अथवा आईपी ठेगानामा प्रणाली/एप्लिकेशनको एकीकृत डाटा व्यवस्थापन केन्द्रमा होस्ट भएको र वास्तविक प्रति रहेको छ।)

The application and database of the above system/s have been properly backed up.

(माथि उल्लिखित प्रणाली/एप्लिकेशन र डाटावेसको व्याकअप लिइएको छ।)

## Annex I: VAPT – Scoping Document

नेटवर्क फायरवाल (\_Network Firewall) र सर्भर हरूको दर सीमा (Rate Limit) लागि अपवादहरू सिर्जना गर्न NCSC को पब्लिक IP (202.45.145.183) व्हाइटलिस्ट मा राखे छौ ।

Official Seal (कार्यालयको छाप)

Name (नाम):

Designation (पद):

Date (मिति):

National Cyber Security Center, Singhadurbar, Kathmandu