त्रिभुवन विश्वविद्यालय/Tribhuvan University

रेसुङ्गा बहुमुखी क्याम्पस

RESUNGA MULTIPLE CAMPUS

तम्घास, गुल्मी
Tamghas, Gulmi

RESUNGA MULTIPLE CAMPUS
TAMGHAS, GULMI
2039

च.नं./Ref.No.: 119
प.सं./Let.No.: 082/083

Date: 2082/08/07

To
Anuj Panthi
Paschimachal Engineering Campus,
Kaski District, Gandaki Pradesh, Nepal

Subject: Authorization and Terms for Conduct of 30 Days External Security Audit

Dear Panthi,

We acknowledge receipt of your formal request dated 3rd Mangsir, 2082 (19th Nov., 2025) seeking authorization to conduct a non-intrusive, external 30-day security audit on the publicly accessible digital systems of Resunga Multiple Campus as a part of your student research and skill-building project.

The administration of Resunga Multiple Campus appreciates your initiative in contributing to our security posture. We are pleased to grant you **authorization to proceed** with the requested audit, subject to the strict adherence of the following terms and conditions:

Terms and Conditions of Authorization

1. **Duration and Scope:**

- Permission is granted for a period of **30 days** starting from 7th Mangsir, 2082 (23rd Nov., 2025).
- The audit must be strictly limited to the publicly exposed digital systems as outlined in your request.
- The audit activities **must strictly follow** the allowed scope of work provided in your request, which includes passive and non-intrusive methods such as OSINT, port scanning, and security header evaluation.

2. **Prohibited Activities (Out-of-Scope):**

- You are **strictly prohibited** from performing any of the activities listed under "Out-of-Scope (Not Performed)," including, but not limited to, exploiting vulnerabilities, password cracking, backend or database access, or conducting DoS/stress testing.

RESUNGA MULTIPLE CAMPUS
TAMGHAS, GULMI
2039

च.नं./Ref.No.: 119
प.सं./Let.No.: 082/083

- No activity shall be destructive, intrusive, or capable of causing performance degradation or system downtime.

3. **Data Integrity and Confidentiality:**

- The audit must not, under any circumstances, affect the integrity, confidentiality, or availability of any data, service, or system belonging to the Campus or its stakeholders.

- All findings, vulnerability data, and audit results are to be treated as **highly Confidential** and must not be shared, discussed, or disclosed to any third party or public forum without the explicit written consent of the Campus Chief.

4. **Reporting and Communication:**

- You must submit a comprehensive, detailed final report of all findings, methodologies used, and recommendations to the Office of the Campus Chief within **7 (seven) days** of the audit conclusion.

- You must immediately notify the Campus Chief (or the designated IT contact) of any critical or high-severity vulnerabilities discovered during the audit.

5. **Liability:**

- The Campus bears no liability for any personal legal or professional consequences arising from activities that violate the agreed-upon scope or any local/national laws.

This authorization confirms permission for non-intrusive research purposes only. Any deviation from the agreed scope or violation of these terms will result in immediate revocation of this permission and may lead to disciplinary action.

We look forward for receiving your findings and recommendations for improving our systems.

....
Surya Upadhya
Campus Chief
Campus Chief