Statement of Work for Network Security Review

Trey Research and Bellows College

# 1. Introduction

This document is a statement of work (SOW) for a network security review project between Trey Research, a consulting firm, and Bellows College, a higher education institution. The purpose of this project is to assess the current state of the network security at Bellows College, identify any vulnerabilities or gaps, and provide recommendations for improvement. The project will be conducted by Trey Research, who will provide the necessary expertise, tools, and methodologies for the network security review. The project will be completed by June 30, 2024, subject to the terms and conditions of this SOW and the contract agreement between the parties.

# 2. Project Phases

The project will consist of four phases: planning, assessment, analysis, and reporting. The following table summarizes the main activities, deliverables, and timelines for each phase.

|  |  |  |  |
| --- | --- | --- | --- |
| Phase | Activities | Deliverables | Timeline |
| Planning | April 20 - April 30, 2024 |  |  |
| Assessment | May 1 - May 31, 2024 |  |  |
| Analysis | June 1 - June 15, 2024 |  |  |
| Reporting | June 16 - June 30, 2024 |  |  |

# 3. Risks and Assumptions

The following are the main risks and assumptions associated with the project:

* The project is dependent on the availability and cooperation of the client's network administrators and users, who will provide access to the network devices and systems, as well as the network policies, procedures, and standards.
* The project is subject to the confidentiality and security requirements of the client, who will grant the necessary permissions and authorizations for the network security review.
* The project is based on the assumption that the network security review will not cause any disruption or damage to the network operations and performance, and that any potential issues will be promptly reported and resolved.
* The project is based on the assumption that the network security review will cover the entire network infrastructure of the client, including the wired and wireless networks, the servers and workstations, the routers and switches, the firewalls and VPNs, and the cloud and web services.
* The project is based on the assumption that the network security review will follow the industry standards and best practices for network security, such as the NIST Cybersecurity Framework, the ISO/IEC 27001, and the CIS Controls.