[College Name]

[IT Department Name]

[Date]

This document confirms that our department has reviewed the presented methods and practices defined by [Replace with 3rd Party Name], on behalf of the [Replace with PI Name] research lab, confirming that they meet or exceed the campus Minimum Security Requirements for Networked Devices, as defined by the Office of Information Security. In addition to the Minimum Security Requirements for Networked Devices, the methods and practices presented also meet or exceed the requirements defined within the [3rd Party Name and Agreement Document] (or henceforth 3rd Party) including, but not limited to, the following areas:

* [Customize to meet requirements outside of minimums as detailed in agreement]
* Regular and auditable system and software updates and security practices
* Use of protection software to prevent external intrusion or compromise attempts
* Campus and local network firewall services to prevent unauthorized external access
* Restricted access and account management in compliance with security standards
* Reduction of unnecessary services and avenues for compromise
* Physical security and controlled access to storage equipment
* Encrypted data storage and transit protections
* Internal-only data storage; no external cloud services
* 3rd Party Data will be securely removed upon the first of either: the completion of the research project requiring the data or the term outlined within the 3rd party data access agreement.

This document is valid for one year from the document date or the period defined within the data access agreement, whichever is longer. The defined research lab is responsible for the implementation, verification, and continual adherence to the proposed practices to ensure compliance for the duration of the required data access, handling, and storage.

Sincerely,