Research Network MOU

## Introduction

Penn State’s institutional data is a mission critical asset. Policies and protections on the network have been crafted to safeguard this data. As technology has evolved, larger data sets, and needs for high speed, low impedance research networks have become a required business need for Penn State to remain competitive in the research space. The intent of a new 10GB research network is to maximize bandwidth available to researchers who have the need for high speed connections in support of their research activities. TNS, RCC, and SOS have worked together to provide 10G networking for researchers. The new network will be referred to as the “Research Network”. TNS will maintain the network, and SOS will provide oversight.

This MOU sets the expectations for the activities and data that are appropriate on this network.

## Purpose

The Research Network is intended to facilitate high-speed movement of data between researchers, compute resources, and physically segregated labs. In addition to the 10G line speeds, this network will employ passive monitoring techniques instead of inline engines, like firewalls, that can introduce latency.

Because TNS will maintain the network, and local departments will not have oversight or the ability to enforce local policy, users of the network will need to agree to abide by behaviors that are consistent with Penn State’s policies and data stewardship expectations.

## Scope

This MOU will apply to the physically separate network known as the Research Network. The expectations set forth apply to the following:

* Onboarding an endpoint to the Research Network (What do I need to do before I can connect an endpoint to the Research Network and how do I get the endpoint connected to the Research Network).
* Security requirements of an endpoint.
* Transferring data to/from an endpoint on the Research Network to/from another network.
* Remote connectivity for management purposes to the endpoint on the Research Network.
* Oversight (TNS and SOS responsibilities).
* Performance and compliance monitoring.
* Compliance.
* Changes to the MOU.

TNS will maintain the network infrastructure and TNS and SOS will work together on the monitoring tools and oversight.

## Onboarding an Endpoint

The principal investigator (PI) is responsible for requesting authorization to use the Research Network. A web form will be available for this purpose (URL here). If the PI will not be the primary person managing the endpoint, then a designated person to whom the PI manages will be named on the request authorization form. The form will be reviewed and approved by Security Operations and Services to ensure compliance with this MOU. The review process will normally take a maximum of one work week, but expedited handling can be requested via the form for time-sensitive research needs.

The PI will certify they accept responsibility for other users in their group that will have access to endpoints on the Research Network. The PI will be responsible for making users aware of this document and enforce its policies and expectations. (Link to quick info sheet?)

The PI to certifies that the endpoint adheres, and will continue to adhere to the Minimum Security Baseline while connected to the Research Network. Because of the high-speed nature of the network, portions of the MSB related to network firewalls are exempted.

The PI is responsible for the acquisition and maintenance of the hardware/software associated with the endpoint connected to the Research Network.

The PI will notify TNS and SOS when the endpoint is removed or decommissioned from the Research Network via an online form *(url here).*

## Security Requirements

The endpoints on this network will need to be solely dedicated to research activities. Use of applications that access Internal or Restricted data not directly related to the approved research project, personal activities, and general administrative activities will not be permitted on this network. Examples of these activities include, but are not limited to: processing grades or other instructional material, accessing payroll or employment applications, and social media.

Endpoints bound to the Research Network will not move back and forth between the Research Network and other networks. The endpoint must have a single network connection to the Research Network only. Any other network connectivity is not permitted on the endpoint.

The researchers will not store, access, or create Internal or Restricted data that are not directly related to the approved research project while using endpoints in the Research Network. AD71 and ADG07 describe the data and provide guidelines for Data Categorization.

Endpoints will be managed in compliance with AD20, the MSB and all other Penn State policies. The MSB requirement for network firewalls is exempted for the Research Network.

## Transfer Data to/from Research Network

Globus Online will be the primary and preferred method of transferring data to/from the Research Network endpoints to/from any other device on/off the Research Network. *(Is this true?) I don’t think so*

Other means to transfer data to/from the Research Network will require submission to and approval from the Security Operations and Services unit.

Let’s discuss remote access and if restrictions (policy or technical) are practical. How does traffic move from RN to something like ISIS?

If you have questions or use cases that you are not sure about, contact SOS at security@psu.edu. *(maybe the RDMZ Jira system would be better?)*

## Remote Connectivity

If remote access to the Research Network is needed from a unit-level system, access must be requested on the initial request form, with the specific network IP addresses that need to access the Research Network endpoint(s) for which the researcher is responsible. Approval will also be necessary from the unit’s Network Contact if unit firewall rules must be modified to facilitate connections.

Wireless access to the Research Network is generally not allowed. Exceptions must be requested by the PI and will normally be facilitated by VPN specific to the Research Network.

See above about remote access, let’s discuss. I’d like to see us favor secure file transfer over things like FTP or HTTP.

If you have questions or use cases that you are not sure about, contact SOS at security@psu.edu. *(maybe the RDMZ Jira system would be better?)*

## Oversight

**Responsibilities of Telecommunications and Networking Services (TNS)**

TNS will ensure that the IP addresses associated with the Research Network are segregated via either router ACL’s or firewall rules from the main academic and administrative networks of the University. The exception would be devices for which Remote Access is authorized one-way from the unit to the Research Network to allow researchers to access their servers from their work environment.

Not sure if this is currently in scope. Let’s figure out the technical options before we make the logical separation in the MOU.

TNS will maintain a web form that will handle the on-boarding and removal of devices from the network. Exceptions to the MSB or unique cases will be reviewed by the RNWG.

TNS will troubleshoot suspected network issues in collaboration with the network contact (WHO IS THAT).

**Responsibilities of Security Operations and Services (SOS)**

SOS will analyze network data and traffic to ensure compliance with the MSB and this MOU.

**Responsibilities of the Network Contact**

The network contact is responsible for working with the researcher to ensure that local policies and guidelines are being followed. The researcher and network contact will need to negotiate support conditions once equipment is moved into the Research network.

## Performance and Compliance Monitoring

The following measures will be in place on the network to monitor performance and compliance with the guidelines in this MOU:

* sFlow Data will be sampled from all switches
* Deep packet inspection is performed on all data that crosses the PSU border

The following tools will be available to address problematic behavior or hardware:

* Deactivation of port to prevent further access to the Research Network
* Border ACLs that prevent access to resources beyond the Penn State border

Development, changes, and growth of the network will be handled by the Research Networking Working Group (RNWG).

## Compliance

SOS will be responsible for the security oversight and notification of violations of this MOU or compromise. The violation notifications will be made to the PI and the Network Contacts.

Let’s talk about the vmhost notification model and firm this up.

The PI is responsible for providing access to the endpoint and credentials for logging into the endpoint in the event of a violation or compromise.

The Network Contacts are responsible for completing the violation or compromise protocols before the endpoint is permitted back on the Research Network.

## Changes to the MOU

Members of the Research Networking Working Group can initiate changes to the MOU. Change proposals will require discussion and approval by the RNWG.

If you have questions or use cases that you are not sure about, contact SOS at security@psu.edu. *(maybe the RDMZ Jira system would be better?)*