Public Infrastructure Security Cyber Education System (PISCES)
Academic Partner Memorandum of Understanding
October 2021

The Public Infrastructure Security Cyber Education System (PISCES) has established a legal and contractual framework to provide infrastructure and data in support of academic courses on cyber security taught by partner institutions. The primary objectives of PISCES are:

a) Facilitate no-cost cybersecurity monitoring for small local governments and the infrastructure they manage;
b) Improve and grow the cybersecurity work force by providing university students with real world experience as cyber analysts to increase their capability and competitive advantage;
c) Encourage university-level research and continuous improvement of the technology stack and methods; and
d) Provide channels to the workforce enhancing placement opportunities for students being taught with the "PISCES experience".

To accomplish these objectives PISCES partners with academic institutions that deliver curated curriculum around real-time data collected from 5-7 local governments through data-sharing agreements. Data collected from these customers using an on-premise device includes network flow data (packet headers only) and alerts from an embedded intrusion detection system (IDS).

Students and instructors from Academic Partners are provided with standard curricula for instruction and student access to the data collected, as provided through the technology stack located at the Washington State Academic Cyber Range, in Poulsbo, WA. Each institution is assigned data streams for 5-7 small communities.

General Understandings

1. PISCES will, through its partnership with Western Washington University (WWU), facilitate the introduction of curated curriculum content, which is designed to provide operational cybersecurity analyst training, as well as provide certain operational tools, techniques, and procedures needed to facilitate the delivery of the curriculum and meeting reporting expectations.

2. PISCES will, through its partnerships with regional local government jurisdictions, maintain data sharing agreements with those organizations, collect network metadata and intrusion detection alerts, and transmit those data to a technology stack located at the Washington State Academic Cyber Range in Poulsbo, Washington. Data collected will represent the real-time activity of approximately 750 government computer users for class analysis.

3. PISCES and its partner government jurisdictions provide wavier of liability for partner academic institutions regarding data and/results of cyber event analysis and reporting except in cases where there is malicious intent.

4. PISCES will, through its partnership with CI Security as the provider of technical services, maintain operation and adequate capacity to facilitate faculty and student access to the live monitoring data, at both the monitoring stack as well as customer premise equipment.

5. PISCES will provide assistance to students seeking job opportunities in positions related to the skills students acquire through participation in the PISCES project. This assistance will vary and may include: job and internship announcements and postings, virtual or physical job fairs, direct introductions to employers, student resume banks, and other activities.

6. Academic Partner agrees to take steps to limit unauthorized access to sensitive data, including establishing guidelines for student use of data, and how data can be accessed. The Academic Partner will enforce access-control at the user and network levels using standard tools and techniques. Academic Partner further agrees to promote and enforce ethical behavior regarding access to customer data.

7. Academic Partner will advertise the class, as appropriate, in their course catalogue.

8. Academic Partner agrees to follow the outlines for the PISCES curricula managed by WWU. The Academic Partner may make minor modifications to the curricula, while maintaining core components. The Academic partner may participate in making recommendations for changes, upgrades, and other edits to the curriculum.

9. Academic Partner agrees to appoint a faculty member to serve as a point of contact for PISCES and the Washington State Academic Cyber Range and to represent the Academic Partner at occasional meetings.

10. Academic Partner agrees to coordinate with PISCES and the Washington State Academic Cyber Range the frequency and timing of course offerings, the number of students in the classes, and other reasonable metrics for the purpose of capacity scaling, and for specific monitoring assignments.

11. Academic Partner agrees to collect and provide adequate information for provisioning student access to the technology stack and data.

12. Academic Partner will require student analysts to sign appropriate non-disclosure agreements, substantially in the form of **Exhibit A** attached hereto and by this reference incorporated herein, committing to protect and not disclose any data and/or information provided by any participating local governmental agency ("AGENCY").
Reproduction and/or disclosure of AGENCY data, associated data, both provided and derived, to include network descriptions and diagrams, AGENCY organization and process, and other data which would divulge the structure of the network, or practices of the AGENCY, for commercial or other purposes, is prohibited, unless expressly authorized through agreement with AGENCY. Anonymization of the data for the purpose of research and research presentation by students is

authorized, provided that the data have been anonymized to the extent that AGENCY is not identified.

13. Academic Partner agrees to anonymize and/or obfuscate representations of the data when making research results public and protect the partner organizations as the source of the data. Both the PISCES Project and Washington State Academic Cyber Range should be acknowledged in any related publications.

14. Academic Partner agrees that any intellectual property developed by students or professors based on participation with PISCES will remain the property of the participating institution unless developed using federal government funds. In such a case, the Intellectual property would be available to the federal government via a royalty free license.

_____   _____
                                                                       Date:

Steve Stein
PISCES-INTL Executive Director

_____   _____

Academic Partner   Date

EXHIBIT A
PISCES Student Nondisclosure Agreement

15. _____(student name) have read the attached Memorandum of Understanding (MOU) between *(academic partner name XXX)* and the PISCES-INTL and will agree to abide by the guidelines set forth in the MOU, especially including Paragraphs 6, 11 and 12. PISCES-INTL is only authorized to receive your name and your *(academic partner)* email address in order to provide access to the necessary monitoring tools for the program. They will not be providing your information to anyone else outside the PISCES program without your prior notification and approval for the purposes described in Paragraph 5 of the MOU.

16. Additionally per Paragraph 12 specifically, *(academic partner)*/PISCES student analysts are required to sign this non-discourse agreement, committing to protect and not disclose any data and/or information provided to PISCES by any participating local governmental agency ("AGENCY"). Moreover, reproduction and/or disclosure of AGENCY data, associated data, both provided and derived, to include network descriptions and diagrams, AGENCY organization and process, and other data which would divulge the structure of the network, or practices of the AGENCY, for commercial or other purposes, is prohibited, unless expressly authorized through agreement with AGENCY. Anonymization of the data for the purpose of research and research presentation by students is authorized, provided that the data have been anonymized to the extent that AGENCY is not identified.

_____

Printed Name

_____   _____

Signature   Date:

**Upon receipt of this signature page, your instructor will provide you with your user name
and password to login to the Cyber Range VPN, the Kibana and MantisBT dashboards.**