Master Information Security Policy & Procedures

International Networks at Indiana University

TransPAC and NEAAR Projects

Version 2.1 - March 2020

Authors: Hans Addleman

Information Security Officer: Hans Addleman

Table of Contents

1 Introduction

This document represents the core information security policies and procedures for the TransPAC and NEAAR projects, including information security-related roles and responsibilities; references to other, special purpose policies; and the core procedures for developing, implementing, and maintaining the information security program.

Our information security program is a structured approach to develop, implement, and maintain an organizational environment conducive to appropriate information security and levels of information-related risk. This program entails ongoing activities to address relevant policies and procedures; technology and mitigations; and training and awareness.

2 Roles & Responsibilities

2.1 Management / Leadership

Dr. Jennifer Schopf is the director of the International Networks at Indiana University (IN@IU) team and has ultimate responsibility for the all IN@IU projects including TransPAC, Networks for European, American, and African Research (NEAAR), and the Engagement and Performance Operations Center (EPOC).

Dr. Jennifer Schopf - 773-294-7320 - jmschopf@iu.edu

2.2 Information Security Officer

IN@IU maintains a position of Information Security Officer (ISO), who reports to the Director of International Networks. The ISO has responsibility for overseeing and coordinating the components of the information security program. The ISO maintains all operative policy and procedure documents, including this document, and will distribute them as appropriate. All reviews of IN@IU-wide policies and procedures are coordinated and archived through this office. The ISO also documents any changes made to the security policy based on these reviews.

The ISO is the first point of contact for any request for clarification of IN@IU information security policy and procedures. The ISO will also coordinate all information security incident responses, including correspondence between the affected staff and users.

As for the date of publication of this document, the Information Security Officer is Hans Addleman. Contact information for the ISO follows:

Hans Addleman - 812-855-3181 - addlema@iu.edu

2.3 Project Personnel and Staff

It is the responsibility of each individual working for IN@IU to review and respect these policies and procedures. It is also the staff member's responsibility to understand the underlying policies that drive those detailed procedures, so that the individual is able to make rational decisions in situations not specifically covered by the detailed procedures.

Each staff member is expected immediately to report any known or suspected violations of security procedures, or known or suspected information security incidents to the ISO or project leadership. In all cases, the staff member and the time of the incident will be documented in order to support a timely analysis of and coordinated response to the situation.

2.4 External Users

TransPAC and NEAAR provide transit networks and have no directly connected users. The AUP's are shared with new partner and peer networks as we stand up new connections:
https://internationalnetworks.iu.edu/files/pdf/policies/TransPAC%20Network%20AUP.pdf
https://internationalnetworks.iu.edu/files/pdf/policies/NEAAR%20Network%20Acceptable%20Use%20Policy.pdf

External users of our network are encouraged to review the privacy policy: https://internationalnetworks.iu.edu/files/pdf/policies/INIU%20Data%20Privacy%20Policy.pdf. All public policies are posted on the IN@IU website (http://internationalnetworks.iu.edu/).

3 Developing, Implementing, and Maintaining Our Cybersecurity Program

3.1 Information Security Risk Management Processes

The IN@IU cybersecurity policies complement and do not overwrite the policies set forth by the Indiana University Information Security (UISO) (https://protect.iu.edu/) office. Information System assets controlled by either Indiana University's University Information Technology Service (UITS) (https://uits.iu.edu/security) or the Indiana University Global Network Operations Center (GlobalNOC) (http://globalnoc.iu.edu/) are governed and secured by the respective organizations. References to these policies can be found in Sections 5 and 7 of this document.

Indiana University has a system wide Enterprise Risk Management framework in place. More information can be found here: https://protect.iu.edu/risk-management/. Indiana University Policy IT-28 (Cyber Risk Mitigation Responsibilities) can be found at http://policies.iu.edu/policies/categories/information-it/it/IT-28.shtml.

3.2 Enforcement

Violations of IN@IU information security policies can result in loss of access to resources and services, and/or disciplinary action. Activities in violation of any laws may be reported to the proper authorities for investigation and prosecution. Anyone who believes that there is a violation of any information security policy or has a related question should contact: irncnoc@globalnoc.iu.edu or 855-476-2662. The IRNC NOC will open a ticket and contact the Information Security Officer. If you are reporting a security incident please follow the IU procedure outlined here: https://protect.iu.edu/online-safety/report-incident/index.html. A quick Incident Response form can be found at https://internationalnetworks.iu.edu/files/pdf/policies/INIU%20Incident%20Response.pdf.

3.3 Modifications to Information Security Policies and Procedures

The Information Security Officer (ISO) is responsible for coordinating changes or additions to established policies and procedures. Requests for changes to established procedures should be presented to the ISO. The ISO will analyze the feasibility and the cost The analysis will be presented to the Director for approval. The ISO upon approval will collaborate with the staff responsible for implementing the recommended change. The Director has final approval over all internal changes to policies and procedures.

4 Resources & Key Contacts

IRNC Network Operations Center (NOC): irncnoc@globalnoc.iu.edu - 855-476-2662
University Information Security Office: uiso@iu.edu - 812-855-8476
University Information Policy Office: uipo@iu.edu - 812-855-8476
Enterprise Risk Management: risk@iu.edu - 317-274-8158
International Networks Security Officer (ISO): addlema@iu.edu 812-855-3181
Director, International Networks: jmschopf@iu.edu

5 Other Policy and Procedure Documents

In addition to this Master document, TransPAC has adopted the following additional policies and procedures.

- Acceptable Use Policy - Indiana University AUP: https://protect.iu.edu/online-safety/acceptable-use.html
- TransPAC Network Acceptable Use Policy - https://internationalnetworks.iu.edu/files/pdf/policies/TransPAC%20Network%20AUP.pdf
- NEAAR Network Acceptable Use Policy - https://internationalnetworks.iu.edu/files/pdf/policies/NEAAR%20Network%20Acceptable%20Use%20Policy.pdf
- GlobalNOC Access Control Policy - The GlobalNOC follows the standard IU UISO standards for access control to managed devices. The specific policies are referenced in Section 7 of this document. The GlobalNOC also employs a AAAA (authentication, authorization, accounting, and audit) infrastructure which is compliant with PCI-DSS policies and specifically monitors system configuration and access changes.
- Asset Management Policy - Indiana University Capital Asset Management Policies: https://fms.iu.edu/capital-assets/policies-and-regulations/
- Information and Information Systems Inventory: https://goo.gl/vr1Uye
- Information Classification Policy - Used to ensure consistency in classification and protection of data. https://internationalnetworks.iu.edu/files/pdf/policies/INIU%20Information%20Classification%20Policy.pdf
- Disaster Recovery Policy - IU and the GlobalNOC both have full disaster recovery plans laid out. The GlobalNOC practices yearly disaster recovery drills.
- Incident Response Procedures - A pre-defined organized approach to addressing and managing a security incident:

https://internationalnetworks.iu.edu/files/pdf/policies/INIU%20Incident%20Response.pdf

- Mobile Computing Policy - Indiana University policy should be followed for securing mobile devices: https://protect.iu.edu/online-safety/hardware-software/index.html
- Password Policy - Indiana University has a password / passphrase policy: https://kb.iu.edu/d/acpu. The GlobalNOC does as well: https://weblogin.grnoc.iu.edu/change-pw/
- Physical [and Environmental] Security Policy - TransPAC equipment is located in the Indiana University Data Center as well as University of Washington's Point of Presence at the Westin Building in Seattle.
    - https://dcops.iu.edu/policies/security.php
- Data Privacy Policy - Privacy and use policy for Netflow data: https://internationalnetworks.iu.edu/files/pdf/policies/INIU%20Data%20Privacy%20Policy.pdf

6 Terms and Acronyms

IU: Indiana University (https://www.iu.edu)
UITS: University Information Technology Services (https://uits.iu.edu/)
IN@IU: International Networks at Indiana University (http://internationalnetworks.iu.edu/)
ISO: Information Security Officer
UISO: University Information Security Office
UIPO: University Information Policy Office
GlobalNOC: Indiana University's Global Network Operations Center (https://globalnoc.iu.edu/)
NEAAR: Networks for European, American, and African Research

7 References and Links

Indiana University IT Policy followed by the GlobalNOC for device access:

- http://policies.iu.edu/policies/categories/information-it/it/IT-01.shtml
- http://policies.iu.edu/policies/categories/information-it/it/IT-02.shtml
- http://policies.iu.edu/policies/categories/information-it/it/IT-03.shtml
- http://policies.iu.edu/policies/categories/information-it/it/IT-07.shtml
- http://policies.iu.edu/policies/categories/information-it/it/IT-11.shtml
- http://policies.iu.edu/policies/categories/information-it/it/IT-12.shtml
- http://policies.iu.edu/policies/categories/information-it/it/IT-18.shtml
- http://policies.iu.edu/policies/categories/information-it/it/IT-19.shtml
- http://policies.iu.edu/policies/categories/information-it/it/IT-20.shtml

- http://policies.iu.edu/policies/categories/information-it/it/IT-21.shtml
- http://policies.iu.edu/policies/categories/information-it/it/IT-28.shtml

***

This document is based in part on
CTSC's Master Information Security Policies & Procedures Template, v2.
For template updates, visit trustedci.org/guide.