Information Classification Policy
International Networks at Indiana University
TransPAC and NEAAR
Version 2.1 - March 2020

Authors: Hans Addleman
Information Security Officer: Hans Addleman

International Networks at Indiana University (IN@IU) has adopted this information classification policy to support the management and protection of information, including electronic data. The classification process is guided by the following rules:

- Asset managers are responsible for assigning classifications to information assets according the standard categories presented below.
- Wherever possible, the information category shall be embedded in and visible on the information itself.
- All IN@IU personnel shall be guided by the information category in their security-related handling of IN@IU information.

For information regarding violations and enforcement, please refer to the IN@IU Master Information Security Policies & Procedures located at https://iu.box.com/v/iniu-master-security.

All IN@IU information and all information entrusted to IN@IU by third parties falls into one of the classification categories in the following table. These categories are presented in order of increasing sensitivity.

Information Classification	**Description**	**Examples**
Public / Unrestricted	Information is not confidential and can be made public without any adverse implications. Temporary loss of availability due to system downtime is an acceptable risk. Integrity is important, but not vital.	• Information widely available in the public domain or for which wide distribution is desirable, e.g., published research results. • SNMP graphs • Router Proxy configurations • Project Reports without financial data
University-Internal / Restricted dsa	Information collected and used by IN@IU staff. Access to this information is restricted to project personnel.	• Partner contact information • Evernote documents and notes • Trello tasks lists • MOUs and Contracts • NSF Project reports
Critical	Information is restricted to management-approved access by specific individuals or classes or role.	• User and root passwords • Netflow records with PII • Employment data with PII