COLUMBIA | SIPA
School of International and Public Affairs

SIPA INFORMATION TECHNOLOGY

CODE OF CONDUCT FOR SIPAIT STAFF

The policy outlines the principles governing the use of computer resources maintained by SIPA Information Technology (SIPA IT) on behalf of SIPA. To ensure that the computing environment is available to satisfy its intended uses, SIPA IT must take appropriate steps to manage and protect its resources. To this end, SIPA IT team members have certain privileges and powers. With these privileges come responsibilities, and this Code of Conduct for SIPA IT team members describes the responsibilities and rights associated with the management of SIPA's computing resources.

Guidelines

These guidelines apply to all professional and student team members, who, in the course of their duties have physical or logical control, custody, or responsibility for components of SIPA's computing environment. Such roles include the following:

System Administrators: Team members possessing appropriate training, certification, or experience who are given privileged access (physically and/or logically) to sensitive information residing on SIPA's computing resources.

Technology Support Staff: Team members who possess a more limited subset of privileges across systems, on specific systems, or within specific applications. The limited subset of privileges provided may include privileges to access sensitive information.

Student Staff: Team members who possess very restricted access to systems and no access to sensitive information except under carefully structured, supervised, and audited circumstances.

Should these guidelines change, all team members will review the change of guidelines and re-submit to these guidelines. In addition, reasonable attempts will be made to communicate the change in guidelines to SIPA IT's clients.

MANAGEMENT RESPONSIBILITIES

- SIPA IT team members must take all reasonable steps to protect systems and their content. Specific requirements are dictated by physical location, connectivity, sensitivity of data, contractual requirements and user characteristics. The term "protect" includes taking appropriate actions to enable systems to meet their intended purposes. Responsibilities include, but are not limited to, those described here. Professional and student team members with limited access only have those responsibilities reasonably under their control and appropriate to their role and level of certification and experience.

- SIPA IT team members must manage computer resources with the intent of meeting their prescribed goals.

- SIPA IT team members must control access as appropriate to specific computer resources. This includes, but is not limited to, ensuring that all access is via appropriate access controls, except those systems with controlled and limited function. Any security vulnerabilities that may allow a user to bypass security must be corrected or managed wherever possible in a prompt manner, and reported to SIPA IT management.

- SIPA IT team members must take reasonable steps to ensure that users do not violate the Computing Guidelines of SIPA. Specifically, facilities and services that allow users to easily bypass security measures of local or remote systems must be minimized.

- SIPA IT team members must respect confidentiality. Data may only be accessed in accordance with the actions outlined in the "Examples of Team Member Actions" section of this document.
- SIPA IT professional staff must structure, supervise, and audit the activities of student staff.

- SIPA IT team members must provide for data backups, hardware maintenance and software maintenance with a view towards providing the greatest benefit to its clients and commensurate with defined goals, business requirements, user needs, and finances.
- SIPA IT team members who observe actual or apparent use, which violates the Computing Guidelines of SIPA, this Code of Conduct, or other applicable computing policies, are obligated to report such use as specified in the section "Privileges and Limits."

SIPA IT team members work hours are scheduled according to their job description and to provide extended support to the SIPA computing community in evenings and weekends, except on University Holidays. If a team member must be absent from work during the work hours for any reason, the staff member must inform the team via e-mail, prior to their absence, if at all possible, and as soon as possible thereafter. Major infractions of the Computing Guidelines of SIPA policy and in particular those related to intrusive or malicious behavior must be reported to the Executive Director of SIPA IT or a duly identified delegate.

PRIVELEGES & LIMITS

In the course of carrying out the preceding responsibilities, SIPA IT team members are empowered to take certain actions. As described in the sections that follow, these actions generally can be taken only under certain circumstances and with due regard for the Computing Guidelines of SIPA policy, users as a whole, and individual users.

In many cases, actions require permission for investigation and reporting of details. Such permission must be obtained from, or reports filed with the Executive Director of SIPA IT.
Certain actions require authorization from and reports filed with SIPA's senior administration or appropriate University functions, where University policy is applicable.

In no case does the granting of privileges confer the absolute right to use the privileges.

System privileges permit the following actions:

Access to systems with privileges exceeding those of a normal user must be restricted to those personnel who specifically require such privileges and have a level of training, certification, or experience appropriate to such privileges.

Within the limitations of the system involved, only those privileges actually required should be granted. It is understood that some systems do not allow granting of certain privileges with fine granularity. In such cases, privileged users may have more rights than they absolutely need. The granting of such privileges does not confer the right to use them.

SIPA IT team members may take all reasonable steps to control the use of and access to SIPA's computing environment. This may include setting access and use priorities and limits, restricting access to and availability of the computing environment, performance management, and making decisions regarding the services to be provided. All such actions and decisions must be made with the conscious requirement to support the intended use of the specific resource and the mission and functions of SIPA.

Data maintained by the system (log files, audit trails) may be used in fulfilling SIPA IT's responsibilities. General release of detailed content of system log files without authorization is prohibited.

System or sub-system failures may yield access without prior permission. In such cases, SIPA IT must act with discretion.

In circumstances where SIPA IT believes that illegal acts or acts violating technology policies are involved, the Executive Director of SIPA Information Technology will be informed and the matter referred to the most appropriate functions of SIPA or the University.

System maintenance, security, integrity or performance issues may indicate that data privacy or system integrity may have been breached, or that system access has been compromised. In such cases, problem analysis will clearly prescribe a course of action. Actions must be reasonably justified. In such cases, prior approval should be obtained from the Executive Director of Information Technology, or, if that is not practical or possible, the action must be reported promptly after the fact.

In exceptional cases not covered by the above points, permission must be obtained from SIPA's senior administration or an appropriate University function where University policy is applicable to carry out actions such as monitoring and investigations that are reasonable given the indicated situation. Such investigations should always be done in such a way as to minimize intrusiveness. Where the threat to SIPA justifies urgent action, and where time would not allow prior consultation, the appropriate member of SIPA's senior administration or an appropriate University function where University policy is applicable must be advised as soon as possible, after the fact. If this member of the senior administration does not agree with the action the administrator may disallow use of any information so obtained.

All actions requiring the permission of senior management or reports according to these guidelines must be logged (electronically or manually). Such logs must be retained for at least one year.

The use and possession of privileges are to be audited and reviewed periodically. Privileges no longer needed by a SIPA IT team member are to be retracted.

In the course of duties, SIPA IT team members may be exposed to or provided confidential, personal, or privileged information. Such information may not be disclosed to others or used for any purpose not authorized by the owner(s) of such information except under the following circumstances:

- There is the reasonable expectation that not reporting the information might result in harm to individuals or SIPA
- The information pertains to acts that are in violation of SIPA or University policies
- The information pertains to acts that are illegal.

In such circumstances, the information should be referred to the Executive Director of SIPA IT for appropriate action.

Examples of Team Member's Actions

In exercising the rights described in this set of guidelines, questions arise as to what SIPA IT team members who are responsible for day-to-day support may do on their own volition, and what actions require permission and/or reporting. These are examples; no claim is made that this is an exhaustive list.

Actions not requiring permission/reporting:

- Data backups
- Systems management (including starting/stopping system, system recovery, repair)
  Systems monitoring where intent is performance management or problem diagnosis
  Controlling systems resource allocation
- Routine mail re-routing and support
- Routine file management (with prior notice if appropriate)
- Scanning systems for viruses
- Scanning systems for potential security holes, including poor passwords
- Statistical analysis for the purpose of system monitoring, performance or utilization

Actions requiring prior notification to user or group owner(s) of data or application:

- Managing the data of terminated employees
- Altering ownership or access rights
- Actions requested by the user: inspection, alteration, or deletion of data owned exclusively by user in support of the user

Actions requiring prior notification to user and user’s reporting relationship:

- Alteration or deletion of user data where policy infractions are suspected. An un-inspected copy of the data may be made prior to notification.

Actions requiring the notification and permission of the Executive Director of SIPA Information Technology or his/her designate:

- Inspection of user data where policy infractions are suspected. An un-inspected copy of the data may be made prior to notification.

- System-wide inspection of user data which includes scanning for copyright violations, programs designed to thwart security (such as password cracking programs), software license verification or other violations of the Acceptable Use Policy.

- Altering data ownership or access rights where system integrity is involved.

- Inspection, alteration or deletion of user data where policy infractions are suspected and potential impact is urgent. System penetration or intrusion will often be present.

- Denial of access to the computing environment for a particular user(s).

Actions resulting in notification of SIPA's senior administration:

- Accessing data for the purposes of identifying potential infractions. Data may be "live" or copied previously.

- Implementation of software to perform automated scanning of user data for violations of computing policies.

In the event that actions are initiated, the involved parties will be notified as soon as is practicable of the nature and scope of the investigation(s).

Agreement

By signing below you state that you have read, understand, and agree to be bound by the terms, duties, and responsibilities described above, as conditions for your employment as a team member of SIPA Information Technology.

Staff Member Name

Staff Member Signature

Supervisor's Name

Supervisor's Signature

Date