COLUMBIA UNIVERSITY

ACCEPTABLE USAGE OF INFORMATION RESOURCES POLICY

Published: October 2013
Revised: November 2014

I. Introduction

This Policy establishes the accountability of all Users (as defined in the Columbia University Information Security Charter (the "Charter")) http://policylibrary.columbia.edu/information-security-charter of Columbia University's Information Resources (as defined in the Charter). It addresses the confidentiality, integrity and availability of such Resources in support of the University's missions, codifies appropriate usage and establishes the need for Users to respect the rights of others and to be in compliance with other University policies, policies of external networks and resources, and all applicable federal, state and local laws and regulations.

The University's Information Resources are provided to support the teaching, learning, clinical and research missions of the University and their supporting administrative functions. Inappropriate use of these Information Resources threatens the atmosphere for the sharing of information, the free exchange of ideas and the security of an environment for creating and maintaining Information Resources.

This Policy applies to the access and use of the University's Information Resources, whether originating from University or non-University Information Resources, including personal computers, as well as the access and use of Information Resources provided by research sponsors to, or leased or hired by, University Users.

Additional terms apply to the use of email at the University, as described in the Columbia University Email Usage Policy http://policylibrary.columbia.edu/email-usage-policy-1**.**

Capitalized terms used herein without definition are defined in the Charter**.**

II. Policy History

The effective date of this Policy is November 1, 2013. This Policy and the other Information Security Policies replace (A) the following University Policies:

- Acceptable Use of IT Resources (Network and Computing) Policy, dated July 1, 2007
- Electronic Information Resources Security Policy, dated March 1, 2007
- Social Security Number (SSN) and Unique Person Number Usage (UPN) Policy, dated September 10, 2007

and (B) the following CUMC Policies:

- Information Security, Backup, Device and Media Controls Policy, dated November 2012.

- Workstation Use and Security Policy, dated November 2102

III. Policy Text

A. Privacy Expectations

The University respects the privacy of individuals and keeps User files and emails on central University Systems as private as possible. However, to protect the integrity of its Information Resources and the rights of all Users, the University reserves the right to monitor access to Information Resources, communications on the University Network and use of Systems and Data, as described in more detail in the Section III(C) of the Charter.

For reasons relating to compliance, security or legal proceedings (e.g., subpoenas) or in an emergency or in exceptional circumstances, the Office of the General Counsel may authorize the reading, blocking or deleting of Data. In particular, in the context of a litigation or an investigation, it may be necessary to access Data with potentially relevant information. Any such action taken must be immediately reported to the Office of the General Counsel and the applicable Information Security Office.

B. Prohibited Actions

No User of Information Resources may take any of the following actions:

1. Use Information Resources in violation of the Information Security Policies;
2. Violate any institutional policies or procedures or use Information Resources for unethical, illegal or criminal purposes;
3. Violate the privacy of co-workers, students, patients, research subjects, alumni(ae) or donors;
4. Violate the rights of any person protected by copyright, trade secret, patent or other intellectual property or similar laws and regulations (i.e., installing or distributing pirated or other inappropriately licensed software);
5. Copy, distribute or transmit copyrighted materials unless authorized;
6. Obstruct University work by consuming excessive amounts of Network bandwidth and other System resources or by deliberately degrading performance of a computer;
7. Create any program, web form or other mechanism that asks for a Columbia user identity and password other than user authentication mechanisms authorized by the applicable Information Security Office;
8. Intimidate, harass, threaten or otherwise do harm to other Users or internal or external Information Resources;
9. Transmit materials in violation of the University's sexual harassment, hostile workplace or protection of minors policies;
10. Make offers of products, items or services that are fraudulent;
11. Intentionally cause a security incident (e.g., log into an account or access Data that the User is not authorized to access, etc.);
12. Intercept or monitor Data not intended for the User unless specifically authorized by the applicable Information Security Office;
13. Attempt to avoid the User authentication or security of Systems or Endpoints;

14. Allow any unauthorized person to use institutional computers for personal use;
15. Violate the policies of external networks and resources while using such external resources;
16. Create or intentionally release computer viruses or worms or otherwise compromise a computer;
17. Engage in frivolous, disruptive or inconsiderate conduct in computer labs or terminal areas; or
18. Use a University network to gain unauthorized access to a System or Data or escalate privileges on a System.

C. Required Actions

Each User of Information Resources must take the following actions:

1. Ensure that his/her account or password is properly used and is not transferred to or used by another individual;
2. Log off from a System or Endpoint after completing access at any location where such System or Endpoint may potentially have multiple Users;
3. Ensure that Sensitive Data is protected with a password and encrypted while in transit or storage;
4. Report the loss or theft of any Endpoint or System containing Sensitive Data in accordance with the Columbia University Electronic Data Security Breach Reporting and Response Policy http://policylibrary.columbia.edu/electronic-data-security-breach-reporting-and-response; and
5. Use University Email Systems only in compliance with the Columbia University Email Usage Policy http://policylibrary.columbia.edu/email-usage-policy-1.

In addition, it is recommended, but not required, that confidential Information be protected with a password while in transit or storage.

IV. Cross References to Related Policies

The Information Security Policies referred to in this Policy are listed in Appendix A hereto.

Appendix A

Related Policies

Electronic Data Security Breach Reporting and Response Policy
http://policylibrary.columbia.edu/electronic-data-security-breach-reporting-and-response

Email Usage Policy
http://policylibrary.columbia.edu/email-usage-policy-1

Information Security Charter
http://policylibrary.columbia.edu/information-security-charter