COLUMBIA UNIVERSITY

REGISTRATION AND PROTECTION OF ENDPOINTS POLICY

Published: October 2013
Revised: November 2014

I. Introduction

This Policy describes the requirements for security controls to protect Endpoints that process, transmit and/or store Data (as each is defined in the Columbia University Information Security Charter (the "Charter")) http://policylibrary.columbia.edu/information-security-charter. Such requirements differ depending on whether such Data is Sensitive Data, Confidential Data, Internal Data or Public Data (as each is defined in the Charter).

No distinction is made in this Policy between an Endpoint owned by the University or personally owned. All Information Security Policies (as defined in the Charter) will apply to a personally owned Endpoint used for University business.

Any Endpoint that processes, transmits and/or stores Data must be registered in accordance with Section III(A) and have the minimum protection requirements set forth in Section III(B) or (C) and, if applicable, Sections III(D), (E), (F) and/or (G), in each case for the most restricted class of Data that is processed, transmitted or stored on such Endpoint.

Capitalized terms used in this Policy 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:

- CUIT Security Policy
- Desktop and Laptop Security Policy, dated November 1, 2007
- Desktop /Laptop/Mobile Devices Security Requirements When Storing Sensitive Data
- Electronic Information Resources Security Policy, dated March 1, 2007
- Encryption Policy, dated December 1, 2007
- Peer to Peer (P2P) File Sharing Policy, dated October 2008
- University Mobile Phone Registration and Password Policy, dated March 1, 2013

and (B) the following CUMC Policies:

- General Information Security Policy, dated November 15, 2007
- Information Security: Media, Backup and Controls, dated November 2012
- Workstation Use and Security Policy, dated November 2012

III. Policy Text

A. Registration of Certain Endpoints

(1) All Endpoints that process, transmit and/or store PHI and (2) all Endpoints that are used for CUMC purposes ("CUMC Endpoints") must be registered with the IT Custodian or other person in a School, Department or business unit who is responsible for maintaining an inventory of Endpoints in his/her area of responsibility. All inventories of registered Endpoints must be provided to the CUMC Information Security Office. Registration will be carried out in accordance with the procedures established by each such IT Custodian or other person.

B. General Protection Requirements for Desktop and Laptop Computers

Each User shall ensure that the following protections, at a minimum, are implemented for each Endpoint that is a desktop or laptop computer:

1. Access to the Endpoint is password protected and conforms to the Columbia University Information Resource Access Control and Log Management Policy http://policylibrary.columbia.edu/information-resource-access-control-and-log-management-policy**.**
2. The Endpoint is running vendor-supported operating systems that are automatically updated and has up-to-date security patches installed.
3. A firewall is activated and configured on the Endpoint.
4. Anti-virus, anti-spyware and monitoring programs are installed to perform continuous and/or scheduled scanning to detect and/or prohibit unauthorized access. The virus definition list is updated at least once daily.
5. The Endpoint is configured to lock after 15 minutes of inactivity.
6. All Data files used for University purposes are backed up regularly**.**
7. The Endpoint is physically protected and not shared with unauthorized persons.
8. Each Endpoint that stores University Data is disposed of in accordance with the Columbia University Sanitization and Disposal of Information Resources Policy http://policylibrary.columbia.edu/sanitization-and-disposal-information-resources-policy**.**

C. General Protection Requirements for Mobile Devices

Each User shall ensure that the following protections, at a minimum, are implemented for each Endpoint that is a Mobile Device:

1. Access to the Endpoint is password protected in accordance with the Columbia University Information Resource Access Control and Log Management Policy http://policylibrary.columbia.edu/information-resource-access-control-and-log-management-policy.
2. The Endpoint contains a mechanism to encrypt all Data stored on the device.
3. The Endpoint is configured to lock after 5 minutes of inactivity.
4. The Endpoint has a mechanism for a secure remote wipe if it is lost or stolen.
5. The Endpoint erases data after 10 failed password or log in attempts.

6. Each Endpoint that stores University Data is disposed of in accordance with the Columbia University Sanitization and Disposal of Information Resources Policy http://policylibrary.columbia.edu/sanitization-and-disposal-information-resources-policy.
7. If the Endpoint is a mobile phone issued or financially subsidized by the University to support its administrative or academic operations, it is the responsibility of departmental administrators (or school or department equivalents) to enter the mobile phone number into People@Columbia (PAC), so that the mobile phone is enrolled in the University's Emergency Text Message Notification System. Please note the following additional points:

    - If the Endpoint is a mobile phone not issued or financially subsidized by the University, it is recommended, but not required, that the Endpoint be enrolled in the University's Emergency Text Message Notification System.
    - If any faculty or staff wish to receive emergency messaging on a different device than their Columbia-issued or subsidized mobile phone, they may log into PAC and change the mobile phone number via PAC Self-Service.

In addition, it is recommended, but not required, that the Endpoint contain a device recovery mechanism through the use of a GPS tracking system.

D. Additional Protection Requirements for CUMC Endpoints

Each User of any CUMC Endpoint must follow the specific provisions relating to Endpoints in the CUMC Information Security Procedures https://secure.cumc.columbia.edu/cumcit/secure/policy/procedures.html.

E. Additional Protection Requirements for Endpoints Containing Sensitive Data or Confidential Data

Each User shall ensure that, in addition to the protections described in Section B or C and Section D above, a record of what Sensitive Data or Confidential Data is stored on each Endpoint is maintained separately from the Endpoint.

In addition, it is recommended but not required, that Confidential Data be protected with password while in transit and in storage.

F. Additional Protection Requirements for Endpoints Containing Sensitive Data

Each User shall ensure that, in addition to the protections described in Section B or C and Sections D and E above, the following protections are implemented for any Endpoint that processes, transmits and/or stores Sensitive Data:

1. Sensitive Data are encrypted while in transit and in storage, including such Data stored on Removable Media.
2. Only encryption technologies that are based on standard algorithms that have no inherent security flaws (e.g., AES, RSA, IDEA, etc.) are used.

3. At a minimum, a 256 bit encryption cipher key is used.
4. If the Endpoint is a desktop or laptop computer, it is encrypted leveraging full disk encryption.
5. The Endpoint does not use Peer-to-Peer Programs unless such use and the configuration of the Program are approved by the applicable Information Security Office.

Any Endpoint that exists on the Effective Date of this Policy and contains PHI, but cannot use encryption because of technology limitations, may be granted a special waiver by the applicable Information Security Office if such Office determines that there are compensating controls in place to address all major information security risks.

G. Additional Protection Requirements for Endpoints Containing EPHI.

Each User shall ensure that, in addition to the protections described in Sections B or C and Sections D, E and F above, the following protections are implemented for any Endpoint that processes, transmits and/or stores EPHI:

1. If the Endpoint is a desktop or laptop computer, it is encrypted leveraging full disk encryption that supports Pre-Boot Authorization.
2. The Endpoint is positioned or shielded so that the Data shown on the screen of the Endpoint is not visible to unauthorized persons.

H. Supplemental Requirements

The requirements lists set forth in this Policy are not comprehensive and supplemental controls may be required by the University to enhance security as necessary.

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

CUMC Information Security Procedures
https://secure.cumc.columbia.edu/cumcit/secure/policy/procedures.html

Information Resource Access Control and Log Management Policy
http://policylibrary.columbia.edu/information-resource-access-control-and-log-management-policy

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

Sanitization and Disposal of Information Resources Policy
http://policylibrary.columbia.edu/sanitization-and-disposal-information-resources-policy