COLUMBIA UNIVERSITY

REGISTRATION AND PROTECTION OF SYSTEMS POLICY

Published: October 2013
Revised: November 2014,
September 2016,
October 2017

I. Introduction

This Policy describes the requirements for security controls to protect Systems 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).

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

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 the following University Policies:

CUIT Publishing Policy
Desktop and Laptop Security Policy, dated November 1, 2007
E-Commerce: Electronic Protection of Credit Card Holder Information Policy, dated June 2008, as amended in August 2009
Electronic Information Server Administrative Policy, dated March 1, 2007
Encryption Policy, dated December 1, 2007
Peer-to-Peer (P2P) File Sharing Policy, dated October 2008

and the following CUMC Policies:

General Information Security Policy, dated November 15, 2007
Information Security: Audit and Evaluation Policy, dated November 15, 2007
Information Security: Media, Backup and Controls, dated November,
2012. System Registration and Certification Policy, dated May 13, 2011.

III. Policy Text

A. Registration of Systems

All Systems, including CUMC Systems, that process, transmit and/or store EPHI/PHI Data must be registered with the CUMC Information Security Office. All Systems that process, transmit and/or store non-EPHI/PHI Sensitive Data and/or Confidential Data must be registered with the CU Information Security Office. Registration will be carried out in accordance with the procedures established by each such Office.

B. General Protection Requirements for Systems

Each System Owner will ensure that the following protections, at a minimum, are implemented for each System:

1. An IT Custodian has been appointed for the System by the System Owner. Contact information for CU Systems has been provided to security@columbia.edu. Contact information for CUMC Systems has been provided to Security@cumc.columbia.edu.
2. The facility that houses the System's Servers, including primary and backup equipment, is environmentally controlled and physically secured from unauthorized access.
3. Each Server is physically labeled with a name or other identification.
4. All Data files on a Server are backed up regularly in accordance with the Columbia University Business Continuity and Disaster Recovery Policy http://policylibrary.columbia.edu/business-continuity-and-disaster-recovery-policy**.**
5. Each of the System's production Servers has a UPS that can provide emergency power and shut the Server down in case of a power outage.
6. Standard configurations, as defined by the applicable Information Security Office, are used to establish a secure configuration baseline.
7. Access to the System's Servers and the Data residing on the System is restricted and is maintained 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.
8. The System's Servers are not used for general desktop functions, such as web browsing, conducting personal email or other Columbia business or non-business functions.
9. The System's Servers are running vendor-supported operating systems and have up-to-date security patches installed.
10. The System's Servers are accessible only for the services provided and only to as much of the Network as is required to provide such services, and firewalls or equivalent protections prevent unauthorized access. To the extent practicable, anti-virus, anti-spyware and System monitoring programs are installed to protect and/or prohibit unauthorized access.
11. Any Peer-to-Peer Program is used only for University purposes, is configured properly as directed by the applicable Information Security Office and does not permit general purpose file sharing over the Internet.
12. Only required services that run on the System's Servers are enabled. Unneeded services are disabled.
13. Each System used for University purposes 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. Additional Protection Requirements for Systems Containing Sensitive Data or Confidential Data

Each System Owner shall ensure that, in addition to the protections described in Section B above, the following protections are implemented for each System that processes, transmits and/or stores Sensitive Data or Confidential Data:

1. A record is kept of what type of Sensitive Data or Confidential Data are stored on the System's Servers and of all changes to the configuration of the Server, and such documentation is kept in a secure, locked location away from the Server.
2. In web-based Systems that are exposed to the Internet, protection mechanisms are implemented to prevent common web-based attacks. Examples of protection elements include web-based firewalls and/or source code security reviews. All such Systems are protected according to the Web Application Security Standard Operating Environment https://cuit.columbia.edu/sites/default/files/content/Web%20Application%20Security%20Standards%20and%20Practices.pdf

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

D. Additional Protection Requirements for Systems Containing Sensitive Data.

Each System Owner shall ensure that, in addition to the protections described in Sections B and C above, the following protections are implemented for each System that processes, transmits and/or stores Sensitive Data:

1. Sensitive Data are encrypted while in transit and in storage, except that Users within CUMC may internally transmit unencrypted EPHI if it is sent to an Approved OHCA Email System.
2. Removable Media containing Sensitive Data are encrypted.
3. In Relational Database Management Systems, Sensitive Data are encrypted in a way that permits database administrators to perform their management functions without access to such Data in a readable format.
4. The System's Servers are maintained in appropriate Data centers, Server closets or Data closets that meet or exceed the following physical requirements:

   Video camera surveillance;
   Badge reader (rather than key) access;
   Use of a visitor log to document all visitors who accompany an authorized User, which is posted by the main ingress/egress point of the secure facility;
   Alarms on the door that alert University Public Safety if (x) the door is left ajar, (y) the door is forced open or (z) the security lock malfunctions; and
   An emergency power shut off button that can cut off power to all circuits in the case of a fire or other physical threat.

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

E. Protection Requirements for Systems in the Columbia Health Care Component

Each System Owner of any System that is part of the Columbia Health Care Component must follow the specific procedures relating to Systems in the CUMC Information Security Procedures https://secure.cumc.columbia.edu/cumcit/secure/policy/procedures.html which reflect the regulatory requirements for managing EPHI.

F. Externally Hosted Systems

Each System Owner shall ensure that the protections described in Section B and, if applicable, Sections C, D and E above are implemented if a externally hosted System (an "Outsourced System") is used. If Sensitive Data are stored on such Outsourced System, the relevant contracts must be approved by the University's Procurement Services and such System's protections must be assessed by the applicable Information Security Office prior to implementation and reassessed on a periodic basis thereafter, as determined by the level of risk.

G. Additional Protections for Email Systems

Each email System Owner shall ensure that, in addition to the protections described in Section B and, if applicable, Sections C, D and E above, or if the email System is an Outsourced System, Section F above, the following protections are implemented for such System:

1. Virus, spam and phishing protection for inbound and outbound messages is implemented through the use of mail filtering software that includes features such as content analysis and real time blacklists.
2. SMTP relay is performed only for authenticated Users or Systems.
3. Monitoring to detect compromised email accounts is implemented and such accounts are disabled on a timely basis.
4. Data loss prevention is implemented to ensure that unencrypted Sensitive Data are transmitted only within the University Network or the CUMC/Hospital OHCA.
5. Detection or prevention mechanisms are implemented to monitor the use of automatic forwarding, redirection or other automated delivery of email as required by the Columbia University Email Usage Policy http://policylibrary.columbia.edu/email-usage-policy-1**.**

H. Additional Protections for Credit Card Information

Each System Owner shall ensure that, in addition to the protections described in Sections B and, if applicable, C, D and E above, or if the credit card processing System is an Outsourced System, Section F above, following protections are implemented for such System:

1. The requirements of the Columbia University Credit Card Acceptance and Processing Policy (the "Credit Card Policy") are complied with.
2. Cardholder Data ("CHD") and Sensitive Authentication Data are not captured, stored, processed or transmitted on University Servers or the University Network other than encrypted CHD through a PCI-validated Point-to-Point-Encryption (P2PE) Solution. Credit cards may not be processed via WiFi.
3. All local IT support groups comply with the requirements of the Merchant Security Review Form referred to in the Credit Card Policy prior to the implementation of or changes to any credit card related services in the merchant environment.
4. All merchant environments are approved by CUIT's PCI Security Group (pcisecurity@columbia.edu).

I. 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.

J. Risk Assessment and Certification Requirements for Systems

In addition to the above requirements, each System that is part of the Columbia Health Care Component is subject to risk assessment by the CUMC Information Security Office, remediation if necessary by the System Owner and certification by the CUMC Information Security Office. Each such System shall be recertified on a periodic basis, as determined by the level of risk, by the CUMC Information Security Office. Each System that processes, transmits and/or stores Sensitive Data (other than EPHI) is subject to risk assessment by the applicable Information Security Office and remediation if necessary by the System Owner. Every Email system must be risk assessed and approved by the applicable Information Security Office.

IV. Cross References to Related Policies and Other Documentation

The Information Security Policies and certain additional documentation referred to in this Policy are listed in Appendix A hereto.

Appendix A

Related Policies and Other Documentation

Business Continuity and Disaster Recovery Policy
http://policylibrary.columbia.edu/business-continuity-and-disaster-recovery-policy

Credit Card Acceptance and Processing Policy
http://policylibrary.columbia.edu/credit-card-acceptance-and-processing-policy

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

Data Classification Policy
http://policylibrary.columbia.edu/data-classification-policy

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

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

List of Approved Vendors
http://finance.columbia.edu/content/e-commerce-gateways

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

Web Application Security Standard Operating Environment
https://cuit.columbia.edu/sites/default/files/content/Web%20Application%20Security%20Standards%20and%20Practices.pdf