COLUMBIA UNIVERSITY
MEDICAL CENTER

Columbia University Medical Center Information Technology

Certified IT Groups

Program Specifications

Columbia University Medical Center
Information Technology
PH 18-109, 630 West 168th Street
New York, NY 10032

General Information

Terms Used in This Document

CAP – Corrective Action Plan

CIO – Chief Information Officer

CISO – Chief Information Security Officer

CUMC – Columbia University Medical Center

CUMC IT – Columbia University Medical Center Information Technology

Client – Refers to a Department in CUMC

Endpoints – Any desktop or laptop computer—Windows, Mac, Linux/UNIX, mobile device, smart phone, tablet, or other portable device used to connect to the University or Medical Center wireless or wired network, access University or Medical Center the information technology resources from any local, remote location, or access any institutional system—CUMC, Columbia University, New York-Presbyterian Hospital, departmental, or individual system, either owned by the University, CUMC, or by an individual and used for the University or CUMC purposes

Security Group (ISG) – CUMC IT/NYP Security Group

Medical Center – Columbia University Medical Center

Server – A Server is a computer that provides a service to other computers, such as processing communications, file storage, or accessing a printing facility. There are many types of Servers including web, database, application, authentication, DNS, mail, proxy, and NTP Servers.

System – A System is a multi-user application or service used for University purposes which resides on one or more computing device(s) and transmits, stores, or processes University data. Any business process and/or application running on a Server is a System. Individual Endpoints are not considered Systems, unless they are performing Server functions.

University – Columbia University

Users – Refers to individuals including but not limited to faculty, staff, students and individuals authorized by the client

Table of Contents

1 Introduction

A key component of the Medical Center's information security plan and risk mitigation strategy, as well as the Corrective Action Plan (CAP) requirements is the creation of the Certified IT Groups program.

Effective March 1, 2015 all the endpoints and systems operating in the Medical Center locations must be under the management of either CUMC IT or a Certified IT Group.

The Certified IT Groups program is set up to validate the qualifications, skills, and experience of the various client IT Groups and their IT Custodians in meeting the framework of the program.

2 Definitions

Term	Description
IT Group	A group of IT personnel who, as full-time employees of the Medical Center or a member of the CUMC OHCA, are responsible for providing a secure infrastructure in support of data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges as authorized by Data Owners or System Owners and implementing and administering controls over data in their respective areas of responsibility. The group of personnel are referred to as IT Custodians in this document. Each IT Group must be led by an IT Manager and contain at least 3 additional technical staff. All IT Custodians must have a direct reporting line to an IT Manager in the same business unit. "Virtual organizations" – where IT Managers and IT Custodians are held together solely through dotted-line reporting structures - are not permitted. Hiring of IT Custodians and IT Managers is the responsibility of the local business unit. The business unit may, but is not obligated to, request assistance from CUMC IT in evaluating IT Manager candidates. Such requests will be fulfilled by CUMC IT on a best-effort basis. Note: Personnel engaged in part-time IT work and part-time other types of activities with IT responsibilities ,such as research, must be be made part of an official IT group to continue their IT-related work. However, as part-timers,

	they do not count toward the three-person IT Group quota required by this policy.
System Owner	The business owner responsible for the system.
IT Custodians	An individual with an undergraduate degree in computer science, related field, or equivalent experience, and with at least two years of experience in a directly comparable technical support role.
IT Manager	A full time manager responsible for the IT Group in a client department. with at least five years' experience in a directly comparable, technical managerial capacity.
Certified IT Groups Leadership Committee	A governance group comprised of five Certified IT Group Managers. The Leadership Committee will meet regularly with the CUMC CIO and CUMC CISO to discuss governance matters.

3 Certification Process

Client IT Groups interested in obtaining the certification are required to submit the evidence and documentation as described under *Section – 4, "Certification Framework,"* to the CUMC Chief Information Officer (CIO) or the CIO's delegate.

The CIO or the CIO's delegate will review the request and the documentation submitted with the request. If necessary additional information will be requested.

After the required information is received, it will go through a combination of audit of the documentation submitted as well as an in-person discussion with the CUMC IT Group Certification Board. The Certification Board comprises of the CUMC CIO, the CIO's delegates, the CUMC CISO, and the CISO's delegates.

Upon the successful completion of the audit and the discussions, the client IT Group will be granted the status of a Certified IT Group..

The CUMC Information Security Office will be responsible for analyzing and certifying that the Certified IT Group is operating in a capacity that is consistent with University Policies and Procedures, as well as operating within an acceptable level of risk, as defined by CUMC Executive Managers.

The Certified IT Group will continue to maintain its status of certification as long as the program principles and procedures as described under *Section – 5, "Program Principles and Procedures"* are adhered to.

4 Loss of Certification

The CUMC IT Group Certification Board may, at its discretion, temporarily suspend or permanently revoke the Certification of any Certified IT Group. Events that could trigger such action include but are not limited to:

- An inability to maintain the staffing requirements noted in section 2, *"Definitions"*
- An ongoing or repeated failure to meet the requirements set forth in this document, regardless of whether this failure was found to be the result of willfull or negligent action.
- An egregious violation of University Policy or CUMC Procedures
- An IT Manager or IT Custodian who engages in a sanctionable offense per the *Sanctions for Unauthorized Access, Use, or Disclosure of Protected Health Information* policy.
- Any other action which the ISO believes creates an unacceptable amount of risk for CUMC

In the unlikely event a suspension or revocation is deemed necessary, the CUMC IT Group Certification Board, in conjunction with the ISO, will conduct a risk assessment and determine an appropriate course of action. This may include:

- **Creation of a "Correction Action Plan" with required changes.** The Certified IT Group would be given an interim Certification with a sunset date set by the CUMC IT Group Certification Board. In the event the requirements of that CAP were not completed within the time specified the Certification would be suspended or revoked.
- **Temporary suspension of IT Certification.** In the event of a temporary suspension the the business unit would be given 30 days to negotiate a temporary support arrangement with another Certified IT group for support.
- **Permanent revocation of IT Certification.** In the event of a permanent revocation the business unit would be given 30 days to transfer their IT support to another Certified IT Group. IT Groups whose Certification is revoked will not be allowed to re-apply for certification for at least 3 years.

5 Certification Framework

Client IT Groups pursuing the certification are required to fulfil the requirements described in this framework and to maintain the certification without any interruption.

Framework Attribute ID	Attribute Description	Details
CITGP-FW-01	IT Resource Requirements	a. A minimum of three IT personnel with a direct report to an IT Manager—a total number of four IT personnel. If the IT Manager is out of the office, the manager's delegate must be qualified to temporarily perform the duties of the IT Manager.
		b. All of the members of the core IT Group must be full-time employees of the Medical Center or another member of the CUMC OHCA. Contractors or consultants from vendor companies can be employed, but are not treated as core members of the IT Group, and so do not count toward the four-person minimum.
CITGP-FW-02	Documentation	

Framework Attribute ID	Attribute Description	Details
	Requirements	a. Evidence that all the IT Custodians in the IT Group have received security training commensurate with their Workforce function. Training materials or guidelines will be provided by the ISO.
		b. List of users in the client department
		c. List of all the endpoints in the client department with their encryption status
		d. List of systems or servers in the client department and their ISO RSAM System Assessment or Certification IDs
		e. Evidence of standard methods of collecting and integrating endpoint inventory data with the CUMC IT Service-Now Configuration Management Database
		f. Vendor production support contracts, warranties, and SLAs for systems or servers in the client department
		g. Scope of Support: A description of the systems, applications, and users that the IT Group is supporting or intends to support. Standard services for Users have been deployed in a secure manner, including desktop management, server management and lab management (Note: Should there be any change in the scope of support, after a group is certified, the Certification Board must be informed.
		h. Evidence that the IT Group has a process for informing the CUMC Information Security Office of any reportable security events or incidents; *Reference:* *http://policylibrary.columbia.edu/electronic-data-security-breach-reporting-and-response-policy-0*
		i. A statement from the IT Manager attesting to the documentation with an affirmative statement that the group will adhere to CU and CUMC information technology policies.
CITGP-FW-03	Hardware and Software Requirements	a. IT Group must ensure that the client department is using hardware and software that is supported in terms of security updates and patches. For example, the IT Group should not be allowing a client department to run a Windows XP computer
		b. IT Group must ensure that the client department is using only the University approved applications, medical devices, or endpoints
CITGP-FW-04		a. Current resumes or profiles of all the IT personnel

Framework Attribute ID	Attribute Description	Details
	IT Group Experience	b. IT Group should submit the support methods or procedures used in the client department for resolving IT incidents. Existing documentation of current practice is sufficient and may be presented in any format convenient for the IT Group.
CITGP-FW-05	Requirements for handling Certified Systems	a. If the Certified IT Group is supporting any Certified Systems, they must fulfil the following requirements in addition to all of the requirements described above:
		b. The IT Group has provided evidence of compliance with the Access Control Policy and Procedures; *Reference:* *http://policylibrary.columbia.edu/information-resource-access-control-and-log-management-policy*
		c. The IT Group has provided evidence that all Managed Systems meet the requirements set forth in the *CUMC System Registration and Protection* Procedures *Reference:* *https://secure.cumc.columbia.edu/cumcit/secure/policy/system.html*
		d. The IT Group has provided evidence that all Managed Endpoints have met the requirements of the *CUMC Endpoint Procedures.* *Reference:* *https://secure.cumc.columbia.edu/cumcit/secure/policy/endpoints.html*
		e. The IT Group has established practices meeting the requirements of the *CU Information Resource Access Control and Log Management Policy* *Reference:* *http://policylibrary.columbia.edu/information-resource-access-control-and-log-management-policy*

Framework Attribute ID	Attribute Description	Details
		f. The IT Group has a business continuity plan and a disaster recovery plan for any Certified Systems *Reference:* *http://policylibrary.columbia.edu/business-continuity-and-disaster-recovery-policy*
		g. The IT Group participates in the CUMC Change Management Process
		h. The IT Group leverages key performance indicators and metrics that measure both operational services and security provided to them by the Certified IT Groups Leadership Committee, and
		i. The IT Group has agreed to provide quarterly status reports to the CUMC Information Security Office on such key performance indicators and metrics, to be developed by the Certified IT Groups Leadership Committee.

6 Certification Program Principles and Procedures

The following are the principles and procedures established for the Certified IT Groups' program.

Principles and Procedure #	Description
CUMC-CITGP-001	Users in CUMC client departments are required to be supported by a Certified IT Group
CUMC-CITGP-002	Certified IT Groups are responsible for managing all endpoints listed in the group's inventory including registering, protecting and proper disposal/decommissioning of systems and assets
CUMC-CITGP-003	IT Custodians must be members of an IT Group
CUMC-CITGP-004	Each IT Group will have an IT Group Manager who is responsible for managing the IT Group
CUMC-CITGP-005	All IT Group Managers will have a dotted line relationship to the CUMC Chief Information Officer (CIO) or the CIO's delegate
CUMC-CITGP-006	IT Groups will implement and adhere to enterprise policies, procedures and standards, defined by the CUMC CIO and the CUMC HIPAA Risk Management Committee, in a consistent and uniform manner, and in concert with CUIT and CUMC IT, as needed
CUMC-CITGP-007	The IT Group Manager must provide management oversight to ensure that the IT Group and its Resources : • Stay up-to-date with requisite training • Adhere to the CU and CUMC information technology policies or procedures • Maintain the standards as defined by the CUMC CIO, CUMC ISO, and the CUMC HIPAA Risk Management Committee.
CUMC-CITGP-008	Certified IT Groups will commit to remaining current on all enterprise policies, procedures and standards by referencing the CUMC Information Security Procedures website frequently to be aware of any new guidance. Lack of knowledge of the CU and CUMC information technology policies or procedures, and standards as defined by the CUMC CIO, CUMC ISO, and the CUMC HIPAA Risk Management Committee cannot be used as a justification for non-compliance. Major, substantive changes to any policies, procedures, or standards will be reviewed by the Certified IT Groups Leadership Committee prior to publication, and communicated to the IT Managers after publication.
CUMC-CITGP-009	The CUMC Information Security Office (ISO) will be responsible for analyzing and certifying that the IT Group is operating in a capacity that is consistent with University Policies and Procedures, as well as operating within an acceptable level of risk, as defined by CUMC Executive Managers

Principles and Procedure #	Description
CUMC-CITGP-010	The CUMC Information Security Office (ISO) may audit certified groups periodically, to ensure that they are conducting their operations within the framework of the certification program
CUMC-CITGP-011	IT Custodians who are not members of a Certified IT Group are not authorized to manage endpoints and systems at CUMC
CUMC-CITGP-012	IT Group Manager or the Group Manager's delegate must attend the monthly CUMC ISO meetings or any other ISO or CUMC IT meetings to which they are invited
CUMC-CITGP-013	IT Groups must manage information security risks pro-actively in the client department they support and must respond immediately to any security issues reported to them by CUMC IT, 24X7, 365 days.
CUMC-CITGP-014	Certified IT Groups will assist the System Owners with Risk Assessments under The Risk Management Program conducted by ISO and any resulting remediation efforts as they apply to IT.
CUMC-CITGP-015	Certified IT Groups will designate a point of contact for general Information Security issues.

Appendix – 1: List of Certified IT Groups

The CUMC CIO and the CUMC HIPAA Risk Management Committee have identified the following IT Groups in the Medical Center and granted them interim certification. If your current IT Groups is not in the list below, it means you have to contact the CUMC CIO's office on how to integrate your IT Group. You may also be contacted to determine how to integrate your group, if you are not in the list below.

ID #	Name
CITGP-01	Budget and Planning IT
CITGP-02	ColumbiaDoctors Information Systems (CDIS)
CITGP-03	College of Dental Medicine (CDM) Clinical Information Services
CITGP-04	Clinical and Translational Science Award (CTSA) IT
CITGP-05	Columbia University Medical Center (CUMC) IT
CITGP-06	Department of Biomedical Informatics (DBMI) IT
CITGP-07	Herbert Irving Comprehensive Cancer Center (HICCC) IT
CITGP-08	Institute of Genomic Medicine IT
CITGP-09	Medicine IT
CITGP-10	Mailman School of Public Health (MSPH) IT
CITGP-11	Neurology IT
CITGP-12	Obstetrics and Gynecology (OBGYN)-Pediatrics IT
CITGP-13	Pathology IT
CITGP-14	Psychiatry IT
CITGP-15	Surgery Computer Operations
CITGP-16	Systems Biology IT (C2B2)
CITGP-17	Web Design Studio (WDS)

Appendix – 2: Policy References

The complete list of Information Security Policies can be found in the University's Administrative Policy Library under:
http://policylibrary.columbia.edu/node_browser/nodes_by_category/term/34

The latest documentation is posted on the CUMC Information Security Procedures website:
https://secure.cumc.columbia.edu/cumcit/secure/policy/procedures.html

The link below is to the document that summarizes all the CUMC Endpoint controls, as the certified IT groups are primarily responsible for implementing them:
https://secure.cumc.columbia.edu/cumcit/secure/security/docs/Endpoint_Controls_Summary.pdf
.

-End of Document-

Columbia University
Medical Center

APPENDIX: BASIC IT SERVICES DESCRIPTION

Background

The Certified IT Group Program Specification includes, as a documentation requirement:

> *"Standard services for Users have been deployed in a secure manner, including desktop management, server management, and lab management."*

This appendix defines a minimum set of "Standard Services."

Certified IT Groups are encouraged to develop clear and complete Service Level Agreements (SLAs) which describe their service offerings. Note that a Certified IT Group does not have to use the naming scheme shown in this document. Providing guidelines for creating SLAs is outside the scope of this document. Groups are welcome to structure their support agreements however they choose as long as the agreements address the areas listed below.

Definition of Standard Services

Basic IT Support

All Certified IT Groups must offer Basic, or "Tier 1" IT service to any department they support. Tier 1 IT service is first-contact support where initial trouble tickets initiate. If the IT group receiving the first point of contact cannot resolve the issue (e.g., if the problem is with an application they do not own) the group must ensure there is a clear handoff or escalation to the proper IT group.

If a Certified IT Group is the *primary* IT group for a department they must offer this Basic IT Support to that department. The primary IT group must keep track of which other IT group provides any *Standard Services* to their department.

General Computer Support

"General Computer Support" refers to support for general-purpose endpoints such as desktops or laptops. This level of support is separate from mobile device support or other specialized endpoint support.

> *Endpoint: any desktop or laptop computer (i.e., Windows, Mac, Linux/Unix), Mobile Device, or other portable device used to connect to the University wireless or wired Network, access Columbia email from any local or remote location, or access any institutional (University, New York-Presbyterian Hospital, departmental, or individual) System either owned by the University or by an individual and used for University purposes.*

Certified IT Groups do not have to provide General Computer Support. If they do, IT groups can choose to provide two support levels – one for University-owned equipment and one for user-owned equipment that is used for work. CITG support offering for either class of endpoints must include the requirements below. If an IT group does not, and is the primary IT group for their department, the group must know which other IT group is supporting their department's endpoints.

If a Certified IT Group offers General Computer Support then the group must ensure supported endpoints operate in a secure manner. The IT group must keep a current inventory of all supported endpoints. All endpoints must meet the relevant CU Policies and CUMC Procedures. These include, at minimum, the Registration and Protection of Endpoints Policy and the Endpoints Procedure. The Certified IT Group will act as the single point-of-contact for any security-related incidents involving any endpoint they support.

The Certified IT Group must provide, at minimum, the following three services for any General Computer Services they offer for University-owned equipment:

1. Troubleshooting and incident or problem resolution for hardware, OS, and supported applications.
2. General maintenance (OS and application patching, upgrades, etc.).
3. Application help for supported applications (how-to, training, etc.).

For endpoints that are not University-owned and access University systems, the Certified IT Group must provide an annual user attestation that declares, at a minimum, that the user is maintaining their equipment per the Registration and Protection of Endpoints Policy and the Endpoints Procedure. The attestation must state at a minimum:

1. Timely OS and application patching, upgrades, and normal maintenance is occurring.
2. Current anti-virus and malware protection is installed.
3. Equipment has been inventoried by the Certified IT Group and up-to-date user contact info provided.
4. Only permitted and actively licensed software is installed.

Certified IT Groups should identify which applications they support. Each IT group should document a path for resolution of issues related to both supported and unsupported applications in their support documentation.

Mobile Device Support

Requirements for Mobile Device Support are the same as for General Computing Support though it is critical to ensure that all Mobile Devices are locked and encrypted. Mobile Device Support is separated out for operational reasons; some IT groups may offer General Computer Support but not provide Mobile Device Support.

> *Mobile Device: a smart/cell phone (e.g., iPhone, Blackberry, Android, Windows phone), tablet (e.g., iPad, Nexus, Galaxy Tab, and other Android based tablet) or USB/removable drive.*

System Support

Certified IT Groups do not have to provide System Support. If they do, their support offering must include the requirements below. A primary IT group for a department that does not provide System Support must know which other Certified IT group is supporting the department's systems.

If a Certified IT Group is providing System Support, the IT Group must ensure the supported systems operate in a secure way. All endpoints must comply with the relevant CU Policies and CUMC Procedures. These include but are not limited to:

- Registration and Protection of Systems Policy
- System Registration and Protection Procedures
- Change Management Process
- Information Security Risk Management Policy
- Sanitization And Disposal Of Information Resources Policy
- Information Resource Access Control And Log Management Policy
- Business Continuity And Disaster Recovery Policy

Refer to the Information Security Charter and CUMC Information Security Procedures for a full list of relevant policies and procedures.

The Certified IT Group will act as the single point-of-contact for any security-related incidents involving system the group supports. The IT group must maintain an inventory of all supported systems.
The Certified IT Group must provide, directly or thru a third party vendor, the following minimum services for any systems they support:

1. Troubleshooting and incident or problem resolution for hardware, virtual infrastructure, OS, and any application components.
2. Installation, configuration, and maintenance of the operating system and any other IT components (applications, databases, etc.).
3. Backup and recovery support.
4. Guidance for security risk assessments and passing security scanning.
5. Registration and maintenance of RSAM records.
6. Application help.
7. Integration with other IT systems (e.g., ensuring the system's authentication against the MC Active Directory domain is working).

If a Certified IT Group does not offer one of the above services for a supported system it must document that gap and know which Certified IT Group provides the necessary support.

> *System: a multi-user application or service used for University purposes which resides on one or more computing device(s) and transmits, stores, or processes University data. Any business process or application running on a Server is a System. Individual Endpoints are not considered Systems, unless they are performing Server functions.*

Specialized IT Support

Specialized IT Support refers to the support of IT components – endpoints or systems – which operate outside the boundaries described above.   Examples of such components include:

- Purpose-built hardware for research.
- Specialized endpoints such as cameras or multimedia devices.
- Embedded or industrial control systems.
- Modalities.

Certified IT Groups do not have to provide Specialized IT Support.   The requirements for such components are often unique, therefore no minimum guidelines for support exist. All IT components, however, must be in compliance with the appropriate Policies and Procedures.