Applicable to

- VUH
- Children's Hospital
- VMG
- VMG Off-site locations
- VPH
- VUSN
- VUSM

Other:

Team Members Performing

- All faculty & staff
- Faculty & staff providing direct patient care or contact
- MD
- House Staff
- APRN/PA
- RN
- LPN

Other:

Lead Author & Content Experts

- Lead Author: Name - Title
  - Content Expert1
  - Content Expert2

SPECIFIC EDUCATION REQUIRED: 

- YES
- NO

Table of Contents

I. Purpose: .................................................................2
II. Policy: ...............................................................2
III. Definitions: ...........................................................2
IV. Specific Information: ...........................................3
V. References: ..........................................................5
VI. Contributors: .......................................................5
VII. Endorsement: .....................................................5
VIII. Approval: ..........................................................5
I. Purpose:

To establish the physical protection and operations of information systems within the Data Center(s) as part of best business practices supporting the confidentiality, integrity, and availability of Vanderbilt University Medical Center (VUMC) information in accordance with federal regulations, including the Health Insurance Accountability and Portability Act (HIPAA).

II. Policy:

While VUMC has an environment of distributed ownership and administration of electronic systems, the physical location for the majority of necessary systems is at least one Data Center. The Informatics Center has the responsibility for the management and configuration of base needs of the Vanderbilt University Hospital Data Center(s). In support of proper operations of a Data Center(s), each application owner and application administrator that requires redundant capacity systems and multiple distribution paths must adhere to the following specification.

III. Definitions:

A. **Computer Operations:** The team of staff managing and controlling the daily operations of the VUMC Data Center

B. **Data Center:** physical space secured to provide a redundant capacity site infrastructure or concurrently maintainable site infrastructure; and provide desired systems with dual paths. This reflects Tier II or III from The Uptime Institute’s Tier Performance Standards. (Our defined data centers containing some portion of VUMC data are: VUH and SunGard)

C. **Data Center Facilities Management (DCFM):** The team responsible for the design and management of all data center facility infrastructure, installation/move/removal of all equipment in the Data Center, capacity measurement/planning of the facilities infrastructure, inventory management, facility monitoring equipment, and hardware maintenance.
IV. Specific Information:

A. Operations

1. Proper and continued operations of a Data Center require specialized training and continued understanding of the configuration of the environment.
2. Data Center Employees are required to be aware and adhere to the current Data Center safety standards and guidelines.
3. Authorized individuals must adhere to all Data Center Facilities Management standards and guidelines when installing, changing, or removing hardware.
4. Full compliance with the Change Management process is required for all work - a formal change or incident ticket will be required for all access encounters other than those of the Computer Operations, DCFM, or Disaster Recovery teams.

B. Access:

1. All Work Force Members authorized access to the Data Center must have a valid Vanderbilt ID and the proper management approval.
2. Access is broken into three levels to support the integrity and physical protection of the systems contained as well as the personal safety of VUMC Work Force Members:
   a. Level 1 – Work Force Members whose job responsibilities are directly related to the daily operations and management of the Data Center. Only these individuals shall have swipe card access.
   b. Level 2 – Work Force Members whose job responsibilities require support of equipment or systems within the Data Center. These individuals shall be required to follow the Change Management processes, and this policy guidelines to register with Computer Operations when entering and existing the Data Center. Each individual must be authorized under DCFM guidelines. These individuals will be required to complete the annual Data Center safety training course.
   c. Level 3 - All other Work Force Members and visitors require approval and authorization for access according to the DCFM guidelines, follow the Change Management processes, this policy guidelines, and must also be escorted by a Level 1 or Level 2 Work Force Member at all times.
3. All other Work Force Members and visitors require approval and authorization for access according to the DCFM guidelines and must also be escorted by a Level 1 or Level 2 Work Force Member at all times.
   a. Limited and/or assisted access may be granted on temporary occasions in order to support systems or applications maintained within the Data Center.
   b. Those visitors/vendors/contractors for work related tasks must be escorted by an authorized individual (Levels 1 or 2).
   c. Visitors and tours of non-work related nature are discouraged. Any visit or tour of this nature must be pre-requested to and pre-approved by Facilities Support. Use the Help Desk for requests.

4. Failure to comply with this policy and the DCFM guidelines may result in loss of access privileges.

C. Responsibilities:

1. The Data Centers have unique design with complex requirements for power, climate control, security, and cabling etc. The DCFM team is responsible for the design, and maintenance of the VUH and SunGard facilities.

2. The Computer Operations team members are responsible for the operations of the VUH Data Center and DCFM is responsible for SunGard.

3. All equipment changes (additions, moves, and/or removals) are required to be processed through Change Control in accordance with established standards.

D. Monitoring:

1. Data Centers are equipped with locked doors requiring card access.

2. DCFM provides monitors and records activities in the Data Center using video surveillance cameras.

3. Computer Operations monitors the door access and registration process for Level 2 and Level 3 access.

4. Additional monitoring of systems and devices may also be present to monitor other items such as power, temperatures, moisture detection, and smoke.
V. References:

Guidelines – Access to SunGard (2nd Data Center)

VI. Contributors:

Lead Author: Monroe Wesley, Director, IT Risk Program / Informatics Security, Informatics Center

Content Experts:
Dave Ellis, Assistant Director, Data Center Facilities Management, Informatics Center
Carl Meadows, Manager, Computer Operations, Informatics Center
Lee Knight
Kevin Chenoweth
Chris Wright
Cheryl Graves
Rick Wheeler

VII. Endorsement:

Operations Policy Committee Date

Luke Gregory Date
Executive Director & CEO
Monroe Carell Jr. Children’s Hospital at Vanderbilt

David Posch Date
CEO, Vanderbilt University Hospital and Clinics
Executive Director, Vanderbilt Medical Group
President, Vanderbilt Integrated Providers

VIII. Approval:

Colleen Conway-Welch PhD, CNM, FAAN, FANCM Date
Nancy & Hilliard Travis Professor of Nursing
Dean, Vanderbilt School of Nursing

Marilyn Dubree MSN, RN, NE-BC Date
Executive Chief Nursing Officer

C. Wright Pinson MBA, MD
Deputy Vice Chancellor for Health Affairs
CEO of the Hospitals and Clinics for VUMC

David Raiford MD
Associate Vice Chancellor for Health Affairs
Senior Associate Dean for Faculty Affairs