I. Introduction

Charles Drew University of Medicine and Science (the University) provides a wide variety of information resources to its faculty, staff, and students, as well as members of the community in order to facilitate the University’s missions of education, research, and service.

The computers, computing systems and networks provided by The University are a shared resource, which requires that all members of the community respect the rights of others and the integrity of the resources, and act responsibly. Protecting the integrity of systems requires that only authorized users have access to information resources, and that resource owners know at all times who has access to their information resources. To protect the integrity of our information resources, this policy has been developed to clearly establish under what circumstances and procedures an individual can be authorized to access University information resources.

II. Scope

University information resources are owned or licensed by the Charles Drew University. Access to them is a privilege for members of the University Community, and carries the obligation of using them responsibly for University related activities. This Access and Authorization Policy for Information Resources applies to all University computing and network resources, as well as all electronic information licensed by the University, including software, journals, databases and books. It applies to all systems owned and maintained by the University Information Resources departments.

III. Policy Statement

Access to University Information Resources is predicated on a valid relationship with the University. Establishing the validity of such relationships is the responsibility of the sponsoring office (HR, Registrar, procurement), or collaborator (for informal research and educational relationships). The “owners” of systems, applications, or resources are the arbiters of access to these systems, applications, or resources, within the general policy described here. The Information Resources departments rely on these sponsoring offices and resource “owners” to authorize user access, and to notify Information Resources departments when access is to be revoked. All Information Resource users have the responsibility to use University resources in an effective, efficient, ethical, and legal manner. Users must agree to the “Rights and
Responsibilities for University Information Resource Users” when they receive an account. Every two years, or when the Rights and Responsibilities agreement is changed, users will be required to re-affirm the agreement.

IV. Procedures

Authorization requirements for University systems

Access to systems managed by the Information Resources departments (Information Systems, Library, Learning Resources etc.) grant access to the network, email, and shared information resources only with specific authorization of responsible parties of record (e.g. HR, Registrar, Procurement) and/or individual system “owners.” Creation of accounts in the University Directory, and basic network, email, and library resource access, can only be authorized by the departments responsible for on-boarding the individuals (HR in the case of employees, Registrar’s office for students, Procurement for Consultants), and only for those with a formal relationship with the University. In addition, each system “owner” is the final arbiter of access for his/her system

System “Owners”

Each information resource owned, subscribed to, or maintained by the University will have a designated individual who is the steward of that information resource. For example the CFO is the “owner” of the financial systems, and has to authorize any user’s access to these systems; Student records systems are “owned” by the Registrar, Donor databases are “owned” by the VP Development, research systems are “owned” by the PI. These individuals are the arbiters of who should or should not have access to their resources. Any request for access to a shared application must be accompanied by authorization from the resource “owner”.

V. Internal Controls and Audit

To ensure that procedures are adhered to, and provide an additional control on access policies, regular reviews of accounts and application access will be conducted.

Network/Phone/Email Account Review

1. Each quarter (or semester for students), a report of current employee and student accounts are generated by the Information Systems department.
2. Human Resources (for employees) and the Registrar’s office (for students) review the list, and note any accounts for individuals that are no longer affiliated with the University, signs it, and returns it to the Information Systems office.
3. IS performs closes accounts as requested based on this list, and reports on completion to the HR or Registrar’s office.
Application Access Review

1. A quarterly report of user access will be given to the resource “owner” for review.
2. The resource “owner” verifies that in all cases users have appropriate access and security levels.
3. If the “owner” finds unauthorized users or inappropriate access, they note these on the list, signs it, and returns it to the Information Systems office.
4. IS performs any requested changes and confirms completion with resource “owner”

VI. Revoking Access

Transitioning roles within the University (as reflected in the Personnel Action Form or equivalent) will trigger a review and reauthorization process for employees to establish what access they need in their new role.

Temporary employees, students, and consultants all will have limited term accounts which reflect their estimated contract length or graduation date at the time of account creation. When these time limits are reached, accounts will be deactivated. Reactivation will require reauthorization of account creation/application access, including new termination date estimates.

Termination of employment, end of contract, or graduation/withdrawal all trigger deactivation of accounts. Student email and student information system access will be extended for a (XXXX?) grace period.

If regular audits of accounts and access reveal unauthorized or undocumented access, those accounts/access will be revoked pending reauthorization.

System “owners” may, at any time, revoke access to their systems to protect data integrity.

If access is revoked, the user may appeal through the established policies for employee, faculty, or student mediation.

Account Creation Procedure

For basic University information resources (network access, file sharing, email etc.), a formal business relationship with the University is required.

New employees:
1. As part of the hiring process, a “Network, Phone and Email Account” request form is prepared and signed by the HR office and signed by the employee’s supervisor. For temporary employees, this form must include an estimated termination date. Any account request for an employee must be signed by an HR officer, who is responsible for verifying employment status with the University.

2. The form is then routed to the Network Administrator in the Information Systems Department and the account created.

3. The Network Administrator delivers a New Account information sheet to the employee with account details and access instructions, and obtains the employee signature on a “Rights and Responsibilities for CDU Computer Users” statement.

New students:

1. As part of the enrollment process, the Registrar’s office prepares a list of new student accounts to be created, attaches this to a filled “Network, Phone and Email account request form,” signs it. This form must include an estimated graduation date. Any account request for a student must be signed by an officer in the Registrar’s office, which is responsible for verifying enrollment status with the University.

2. The form is then routed to the Network Administrator in the Information Systems Department and the account created.

3. The Network Administrator delivers a New Account information sheets and “Rights and Responsibilities for CDU Computer Users” statements for each student to the Registrar’s office.

4. Students must sign their statements before receiving their account information from the Registrar’s office.

5. The Registrar returns signed statements to the Network Administrator.

Consultants:

1. The Department/Unit Director hiring the consultant prepares a “Network, Phone and Email account request form,” and signs it. This form must include a termination date for the contract.

2. The form must be signed by an officer in the Procurement office, which is responsible for verifying that the consultant has a valid contract status with the University, and that the scope of work requires the accounts requested.

3. The form is then routed to the Network Administrator in the Information Systems Department and the account created.

4. The Network Administrator delivers a New Account information sheet to the consultant with account details and access instructions, and obtains the consultant signature on a “Rights and Responsibilities for CDU Computer Users” statement.

**Application Access Procedure**

Access to applications may first require a network/email account to be established following the “Account Creation Procedure” above. Informal collaborators may be
granted access to specific research and educational applications only within the scope of their collaboration, and at the written request of the PI or Program Director.

Employees:

4. The employee’s supervisor prepares and signs an “Application Access Form” which describes the specific application modules and levels of access an employee should be granted. For temporary employees, a termination date must be included.

5. If the supervisor is not the resource “owner”, it is then routed to the “owner” for authorization, and any additional limitations on access that the “owner” believes should be applied.

6. It is then routed to the Network Administrator in the Information Systems Department and the account access created.

7. The Network Administrator delivers a New Account information sheet to the employee with account details and access instructions, and provides a copy to the resource “owner”.

Students:

6. The Registrar’s office (or the student’s supervisor if access is for a work study position) prepares an “Application Access Form” and signs it. This form must include an estimated graduation date or end date for the work study assignment.

7. If the Registrar or supervisor is not the resource “owner”, the form is then routed to the “owner” for authorization, and any additional limitations on access that the “owner” believes should be applied.

8. It is then routed to the Network Administrator in the Information Systems Department and the account access created.

9. The Network Administrator delivers a New Account information sheet to the employee with account details and access instructions, and provides a copy to the resource “owner”.

Consultants:

5. The Department/Unit Director hiring the consultant prepares a “Application Access Form,” and signs it. This form must include a termination date for the contract.

6. The form must be signed by an officer in the Procurement office, which is responsible for verifying that the consultant has a valid contract status with the University, and that the scope of work requires the access requested.

7. If the Department/Unit Director is not the resource “owner”, the form is then routed to the “owner” for authorization, and any additional limitations on access that the “owner” believes should be applied.

8. It is then routed to the Network Administrator in the Information Systems Department and the account access created.

9. The Network Administrator delivers a New Account information sheet to the employee with account details and access instructions, and provides a copy to the resource “owner”.