2022

DILLARD UNIVERSITY

ITT Policy and Procedures Manual

HELPDESK@DILLARD.EDU
HOWARD HOUSE
(504)816-4716

Table of Contents

Purpose and Scope

Information Technology and Telecommunications (ITT) is the departmental agency that manages Dillard University's technology based services. As a service organization, ITT is charged with the responsibility of providing leading edge technological and appropriate tools to support the needs of academic and administrative entities in a cost effective and user friendly environment. As a support organization, we must adhere to the larger goal of connecting our users to other people/organizations, their work, their studies, and information and training resources. In supporting the priorities and directives of the DU administration, ITT plays a critical cog in the Universities efforts to make the attainment of a college degree affordable, accessible and relevant to our current and future students.

This document sets forth the University's policy regarding access to and the use of any computing or network resource owned, operated or otherwise provided to users by Dillard University. The Dillard University resources include Wi-Fi, Cable TV services, traditional voice services, cellular voice and messaging service, and access facilities.

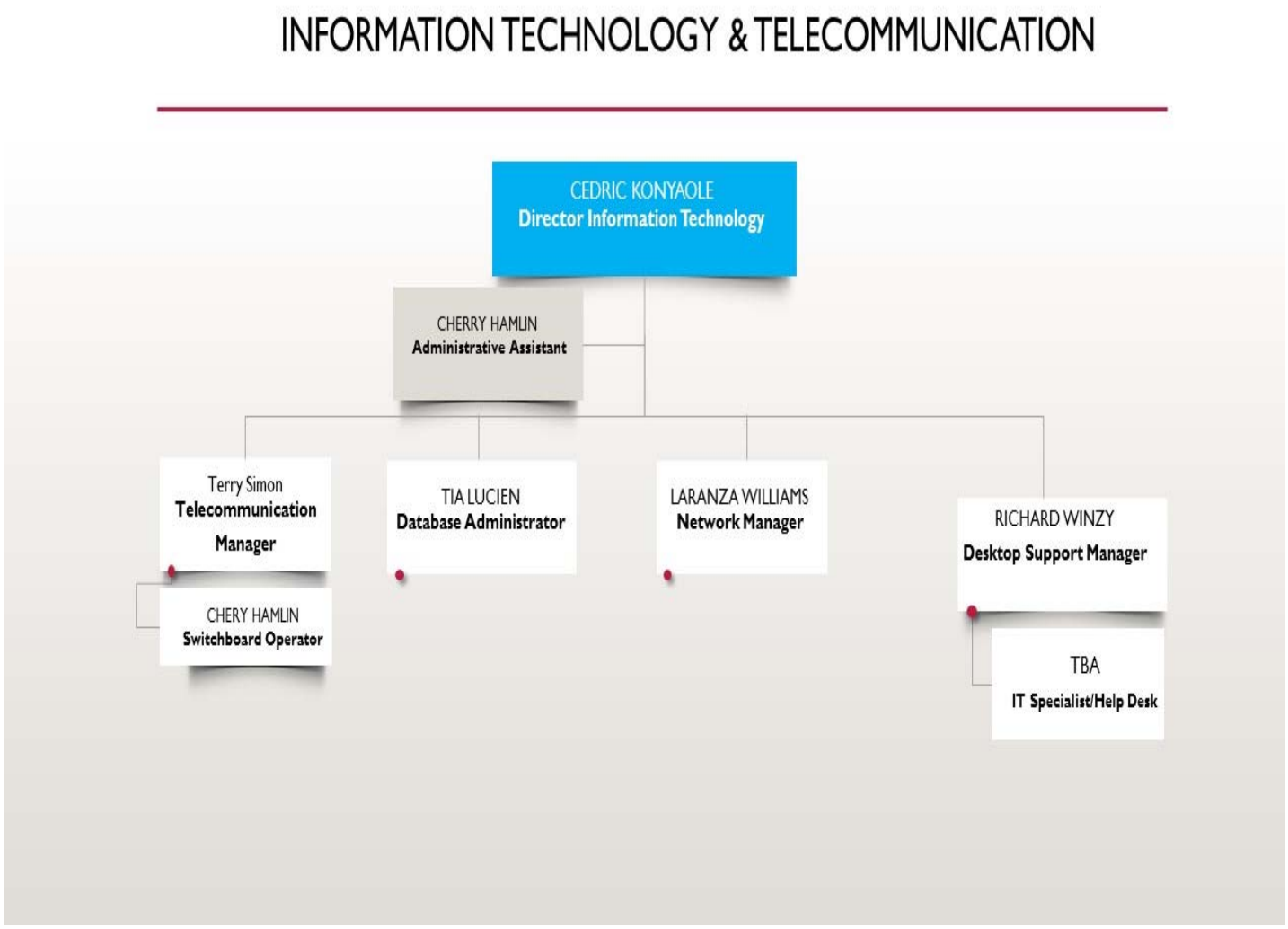
Computer and network users at Dillard University must demonstrate proficiency in the proper, ethical, and legal use of computing and network resources provided by the University. Nothing in this policy superseded federal, state and local laws and regulations pertaining to the use of computing & network resources.

The University reserves the right to change this policy in response to altered or unanticipated circumstances.

Any questions concerning computing or network policies at Dillard University not resolved by this document should be directed to:

Cedric Konyaole
Director of Information Technology & Telecommunications
Howard House Room 110
504-816-4872

Organizational Chart



Roles and Responsibilities of ITT

Director of Information Technology:

- Responsible for the planning, organizing, and execution of all IT functions. This includes directing all IT operations to meet the university community needs as well as the support and maintenance of existing applications and development of new technical solutions.
- Provide the vision and leadership for designing, developing and implementing a network infrastructure as well as disaster recovery systems and processes.
- Overseeing technical projects in alignment with organizational goals.

Database Administrator/SQL Developer:

The primary purpose of a Database Administrator is to develop database systems solutions, related master files, and associated technical services designed to support client business objectives through data analysis, modeling, and management.

Telecommunications Manager:

Responsible for the strategic planning, design, maintenance and implementation of the university telecommunications systems which includes voice systems, cable TV, ISP provider, RFP Bids, and smart technology for the classroom.

Network Infrastructure Manager:

- Responsible for installing, configuring, and maintain the university network infrastructure as well as network performance monitoring which includes, switches, routers, security appliances, wireless controllers, ups systems and BYOD appliance.
- Identify and maintain upgrades to the network.
- Diagnosing and fixing problems or potential problems with the network and its hardware, software and systems.

Desktop & Server Support Manager:

- Responsible for the smooth operation with the assistance of the helpdesk technician whose primary function is to help customers resolve issues with their desktop computers.
- Responsible for approval of all software & hardware used University wide. All Equipment quotes must be approved by Desktop & Server Support Manager.
- The central point of contact for all IT related incidents and service requests. Provide a second line of support for all faculty, staff and students. Implement and maintain all network & virtual servers.

IT Specialist/Desktop Support:

- Provide the first line of support and contact for students, faculty and staff seeking technical assistance in person, over the phone or by email.
- Install, modify, and repair computer hardware and software.
- Performing remote troubleshooting through diagnostic procedures and pertinent questions.
- Responsible for on-site installation, implementation, maintenance, troubleshooting, and repair of the university multi-vendor systems solution that include hardware, software, applications, printers, and servers.

Switch Board Operator/Administrative Assistance:

- Responsible for answering all incoming calls to the university, greeting callers, providing information, transferring calls and/or taking messages as necessary.
- Order supplies, take minutes during meetings, entering requisitions, and whatever duties that are needed by the director of IT.

Computer and Network Security User Policies

Authorized Access

Only persons properly authorized may access the University's network or computer facilities. Proper authorization is provided to ITT by Human Resources in conjunction with the hiring process for faculty and staff and by the Registrar's office for students. Exceptions to the above require VP level approval.

Upon approval all faculty, staff, and students are assigned an e-mail account that becomes part of the University's Administrative Database (Jenzabar). The data must be entered into the Jenzabar to verify initial eligibility for an account, to obtain a unique permanent ID, and to learn of any change of status which signals that an account should be removed.

Individual faculty, staff, or students must verify that they are correctly represented in the database and request any needed corrections.

Shall the status change of a person from Jenzabar will result in termination of the account. Typically, such removals result from resignation, termination, or students who are no longer enrolled.

Short-term accounts may be authorized to meet particular needs. These normally require a faculty/staff sponsor to be responsible for use under the temporary account and require approval through the appropriate department head.

Authorized Activities

Dillard University provides computing and network resources to faculty, staff, and students for their use in academic, administrative, and social enrichment. Personal exploration and enrichment that does not conflict with the Universities Mission or any applicable laws is acceptable.

As with any finite resource prudent usage is mandated. Policies described in this document seek to facilitate usage directly related to the academic and administrative missions of the University, limit secondary use to times when no primary uses will be adversely affected, and eliminate illegal or abusive usage. In addition, policies are included to help maintain an ethical and amicable working environment for users.

Usage that results in specific, substantiated complaints from another user and/or user body will result in a re-evaluation of that activity.

Any personal, for profit activity or any activity that competes with University Business is prohibit.

Use of the University computing facilities on behalf of any organization, even non-profit organizations or Dillard-Affiliated Organizations require prior approval by the Dillard University Administration. If you are uncertain whether a specific activity is acceptable, discuss your concerns with an administrator or with ITT.

Other Usage

The computing and network applications that enable student, staff, and/or faculty to meet the recognized education, research, and administrative goals of the University have priority.

It is the responsibility of ITT to properly size all facilities to usage and economic realities we face at Dillard University. With that in mind, academic and/or administrative functions take precedence over any other usage. Use of limited resources should be minimized or deferred until times when they will not interfere with the Universities' primary functions.

Other uses are proper only if the resources are not otherwise needed, and the use is not prohibited by other governing issues. In determining whether your proposed activities will adversely affect other users, consider network traffic and restrictions on simultaneous use of any resource (e.g., ports, licenses) as well as competition for the particular system/systems you want to use. If your non-primary application, whether by delayed response times or any other factor, then your use should be deferred until later. (Using resources to play games or download music do not have priority over students that have a need to complete assignments)

Integrity

Users are presumed to be responsible for all activity pertaining to their account. Do not allow anyone else to use your account. Release of access passwords to non-authorized persons is a direct violation of University policy. If you need to share files, contact the ITT helpdesk at 816.4716 or **helpdesk@dillard.edu**

Users who make deliberate attempts to hide their identities from other users or system administrators are in violation of University policy.

Users may be required to show a valid Dillard University ID card to obtain access to computing and network facilities or to pick up printed materials.

Users who attempt to crash or subvert security, scan or map the network, or otherwise adversely affect operations on any system are in violation of University policy and possibly in violation of various federal and state laws. Violators will be subject to University based disciplinary action and civil action at the discretion of University officials.

Conduct

Users may not harass or threaten other users, attempt to steal password, files or other user/system information, attempt to crash, violate the integrity of, or adversely affect the activities of a computer system or network. Distasteful or offensive displays, messages, and documents are not permitted inclusive of IMS type messaging originated or terminated utilizing Dillard University facilities. Actions that adversely affect the working environment of other users are not acceptable. Physical abuse, mishandling and modification of computers, printers and other hardware are not permitted.

Waste

Unnecessary storage of files, careless execution of high resource consuming programs, or generation of excessive printed output id wasteful. When any process is consuming excessive system resources or is objectionably degrading system response it may be terminated, or its priority may be change, without notice. Users should also be aware that hard copy output devices are expensive to operate ant that wasteful use of such devices may result in charges to the account that requested the output. Sending chain letters or unwanted e-mail is to be discouraged.

Electronic Publication

Posting to an Internet discussion group or displaying personal web pages are forms of electronic publication. Electronic publications can be created so easily that checks and balances that help produce responsibility in print media may not operate until it is too late.

Users are responsible for the content and the consequences of their electronic publications. Various local, state and federal laws (such as, but not limited to copyright, obscenity and libel) may apply, as may the laws of other jurisdictions or countries. Acceptable usage may also depend on your intended audience or whether a minor can access your publication.

Because anything you place on the Internet from Dillard University can easily be determined to have originated on a device connected to the University's network some of your readers may assume that your publication is sponsored by the University. Unless you have such authority, you should include a disclaimer on your publication. Do not use official Dillard University logos or seals unless you are specifically authorized to do so. Information posted using an official logo or seal without proper authorization will be removed.

If you expect to publish something that will attract heavy responses, you should discuss it with your department head and an ITT representative. Heavy responses can overburden system resources requiring publishing modifications if required.

Licensing and Contracts:

The University normally acquires hardware, software and other services under educational agreements that often restrict the usage of said items. Substantial fines are levied for violation of agreements that restrict items such as duplication, source code and simultaneous users. Users are required to honor all University initiated contractual agreements with violations subject to disciplinary discretion by the Administration.

Privacy & Monitoring

Although system administrators are co-owners of all user files, the University recognizes that faculty, staff and students have a substantial interest in privacy with regard to their computing activities, even when those activities involve only University business.

The University will not monitor user transactions or the content of user files as a routine matter. It will monitor traffic for usage and most frequented visited sites on the web and will respond to legal process. It may inspect without notice the contents of files in the course of the investigation triggered by indications of impropriety, to resolve system problems or to locate substantive University related information that is not available by less intrusive means.

It is a violation of University policy for any employee, including system administrators and supervisors, to use the computing systems to satisfy idle curiosity about the affairs of others with no substantial purpose for obtaining access to the files or communications of others.

Grounds for Examination of Users' files

Circumstances that may require a system administrator to inspect the contents of files created and/or maintained by University faculty staff or students are:

- A search warrant or subpoena specifically pertaining to user files, served by law enforcement.
- A reason to believe that the file is connected with violations of University policy or state or federal law.
- An investigation of a specific, substantiated complaint by another user, either at the University or at another site about activities originating from a Dillard University user's account.
- An urgent need, by a supervisor or project administrator, to access critical University information which is maintained by one of his/her staff or project members and which cannot be obtained by less intrusive means.

Such circumstances are reviewed and approved in writing by the head of the department or his/her designee in which the computing system is located prior to granting access.
Users should also be aware that system administrators might view the contents of a file during routine system operations.

Campus Computer Laboratory Use Polices

It is our pleasure to welcome you to Dillard's Open Computer Labs. Our mission is to provide the end user with computing resources, hardware, software and a capable staff to help users excel in their academic pursuits. ITT provides two virtual labs one located in DUCIEF Room 101 & Howard House Room 109. All other labs are controlled by individual departments. Howard House 109 is open for use Monday – Friday 8:00 a.m. until 5:00p.m

Laboratory Use Policies

- Users must have a Dillard University assigned user account to gain access to the computers in the open labs. (Limited access is provided to official university visitors with advanced notice).
- All students, faculty and staff are required to present proper identification when using facilities.
- Users are responsible for saving their documents on their own storage devices (USB or CD-ROM).
- Saving documents or files to the system hard drive is not allowed. Files saved to the desktop or hard drive will be lost when the computers are logged off or restarted.
- When listening to audio on lab computers user supplied headphones are to be used.
- Downloading or installing programs on the hard drives is strictly prohibited.
- Recreational computer use is prohibited during the weeks of mid-terms and final examinations.
- Lab assistants should be informed of any hardware/software difficulties. Do not attempt to correct these problems yourself.
- In the event of an emergency, please exit the labs as quickly as possible. Liability
- Lab personnel are not responsible for lost items. (Users may check with lab personnel for items that may have been turned into the office or found).

- The university is not responsible for lost data; we will make every effort to assist users in the retrieval process.
- No food, drink or pets are permitted in labs under any circumstances.
- Cell phone use is strictly prohibited in university computer labs.
- The labs are academic study areas and noise must be kept to a minimum.
- Users in noncompliance of rules will be asked to leave.
- Campus Police will be called if a user refuses to abide by university regulations.
- User removed from the lab may discuss his/her case with lab management.
- Obvious disregard of listed policies can result in loss of user privileges.

Jenzabar Access Policy

Policy #	Origination Date	Responsible Office	Status	Approval Date
22-08F-02	7.26.2022	ITT	DRAFT	

Policy Statement

This policy will establish training for each user's designated module within Jenzabar before access is given to help improve the state of the University's Student Information System (SIS)

Reason for Policy/Purpose

The reason for this policy is to improve the information stored in the University's SIS and enhance both Faculty & Staff knowledge of the functions within their department's module.

Who Needs to Know This Policy

All Dillard Faculty and Staff.

Table of Contents

Definitions

Definitions of the terms used in this policy.

Term	Definition
Student Information System (SIS)	Is a computer system that manages a range of information about Dillard students

Play Database	Test Environment of SIS (Jenzabar)
Production Database	Live Environment of SIS (Jenzabar)

Responsibilities	
Office	Responsibility
ITT	Responsible for ensuring users have access to both Google Meets & Microsoft Teams
Dillard Faculty & Staff	are responsible for adhering to this policy and completing the required training for their Module to have access to Jenzabar

Policy/Procedures

Policy

When requesting access to the University's Student Information System (Jenzabar) the user will only receive access to the Play Database. Upon completion of the user's module training, they will need to provide the certificate to helpdesk@dillard.edu to receive access to the Production Database.

Existing users will have until close of business October 14, 2022, to produce the certificate of completion for their module's training or access to the Production Database will be revoked.

Website Address(s) for this Policy

The web address for this policy is not final, discussions with the Office of Communication and Marketing are ongoing.

Contact(s)

For questions about this policy contact:

Tia Lucien
504.816.4521
tlucien@dillard.edu

Related Information

SOP and instructions will be posted with the policy.

Who Approved this Policy

Pending approval from the University President and Legal Counsel.

History/Revision Dates

Origination Date: 7.26.2022

Approval Date:

Updated:

Revised: **Next Review Date:**

Network Security Policy

Purpose

Dillard University resources, such as its Internet/Intranet systems, is to be used for Dillard business purposes in serving the interests of the University.

The participation and support of every student, faculty, employee and affiliate who deals with information and/or information systems is necessary to achieve effective security. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to delineate acceptable use of Dillard University technology resources. These rules are in place to protect the user of these resources and the University. Inappropriate use exposes Dillard University to risks including malware/virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to all Dillard University networks, both the perimeter and the infrastructure, and the parties with which we do businesses.

Maintenance

This Policy will be reviewed by the Dillard University Information Security Office annually or as deemed, appropriate based on changes in technology or regulatory requirements.

Enforcement

Violations of this Policy may result in suspension or loss of the violator's use privileges, with respect to the University-owned Information Systems. Additional administrative sanctions may apply; up to and including termination of employment or contractor status with the University, or expulsion of student workers. Civil, criminal and equitable remedies may also apply.

Exceptions

Exceptions to this Policy must be approved by the information Security Office, under the guidance of the University's Provost, or Vice President of Business and Finance. All exceptions will be documented. Policy exceptions will be reviewed on a periodic basis for appropriate access and use.

Policy

The data network is a shared resource used by the entire University community and its affiliates in support of the business processes and academic missions. Business units and community members must cooperate to protect the network by securing computers and network devices in order to secure access.

The following rules define the Dillard policy regarding access to the University network:

1. Only authorized personnel can gain access to Dillard University network. Positive identification is required for system usage. All users must have their identities positively identified with user-IDs and secure passwords--or by other means that provide equal or greater security--prior to being permitted to use the network.

2. User-IDs must each uniquely identify a single user. Each computer user-ID must uniquely identify only one user, so as to ensure individual accountability in system logs. Shared or group user-IDs are not permitted.

3. Use of service accounts for local log-ins by any individual is prohibited. All local accounts are managed by IT staff only. This rule is designed to prevent unauthorized changes to production data by accounts that allow groups of users to employ the same password. In cases where users require authorities inherent in service accounts, the user's manager must obtain approval from ITT. Those privileges may be assigned to individual users on as-needed basis and must be revoked when they are no longer necessary or employed with the university.

4. Multiple simultaneous remote external network connections are prohibited. Unless special permission has been granted by the Director of Information Technology.

5. All users must log off before leaving sensitive systems unattended. If the computer system to which users are connected or which they are currently using contains sensitive information, and especially if they have special access rights, such as domain admin or system administrator privileges, users must not leave their computer, workstation, or terminal unattended without first logging-out, locking the workstation, or invoking a password-protected screen saver.

6. ITT Staff supporting the university network must follow:

    A. Policies and procedures to validate firewall activation, operating system installation, application software security patches and virus protection updates for all devices in the unit's areas of physical or administrative control that are to be configured to utilize network resources that are being controlled and managed by IT Staff
    B. The IT staff must retain all documentation for audits as long as the device is in operation. Any connection to the Internet, or to a national or regional network from a private network operated by an academic, administrative, or support unit, must be made via University network resources.

C. All network access attempts (success or failure) must be logged and retained for auditing.

D. All Servers are maintained both by IT Staff and MYIT contracting service provider. At a minimum the following information is required to identify the point of contact:

1. Server contact(s) and location, and a backup contact
2. Hardware and Operating System/Version
3. Main functions and applications, if applicable
4. Information in the Enterprise Management System must be kept up-to-date.
5. All service tags must be inventoried and warranties kept current.

E. The following items serve as provisioning configuration guidelines for the Servers that are managed by DU IT Staff and MYIT:

1. Services and applications that will not be used must be disabled where practical.
2. Access to services should be logged and/or protected through access-control methods such as Transmission Control Protocol (TCP) Wrappers.
3. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
4. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is available.
5. Do not use root account when a non-privileged account can perform the task.
6. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPsec).
7. The University servers are physically located in an access-controlled environment with an access controlled key-pad entry lock.
8. DHCP IP addresses must not be publicly released.

F. Each device must meet the following minimum standards prior to, and after connecting to the data network or support infrastructure:

1. The device must be guarded by an up-to-date and active firewall set to protect it from unauthorized network traffic.
2. Current operating system and application software with current security patches must be installed.
3. The device must be protected against malicious or undesired software such as viruses, spyware, or adware.
4. Access to the device must require appropriate authentication controls such as account identifiers and robust passwords.

G. All connections between Dillard University internal network and the Internet outside (or any other publicly accessible computer network) is protected by **Sonic Wall NSA 5700 Security Appliance and Crowd-Strike Falcon Cloud Cybersecurity Endpoint Complete Protection Platform.**

H. The current outside University Web Server is being outsource and the university requires the outsource vendor to adhere to all policies regarding firewall and virus protection services.

VPN ACCESS

Approved employees and authorized third parties (customers, vendors, etc.) may utilize the benefit of VPN, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the Remote Access Policy.

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to internal networks.
2. When actively connected to the enterprise network, the VPN will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
3. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
4. VPN gateways will be set up and managed by DU IT Staff and MYIT
5. All computers connected to the internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the enterprise standard, this includes personal computer.
6. VPN users will be automatically disconnected from the network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
7. Users of computers that are not owned by the University must configure the equipment to comply with VPN and Network policies. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the network, and as such are subject to the same rules and regulations that apply to the University's owned equipment, i.e., their machines must be configured to comply with the University security policies.

I. REMOTE ACCESS

1. Secure remote access is strictly controlled. Control enforced via one-time password authentication or public/private key with strong passphrases.
2. At no time should any employee provide his or her login or email password to anyone, not even family members.
3. Employees and contractors with remote access privileges must ensure that their University owned or personal computer or workstation, which remotely connected to the enterprise network, not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Employees, contractors and students with remote access privileges to the enterprise network must not use non-University email accounts or other external resources to conduct University business.
5. Recon$_{fi}$guration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time
6. All hosts that are connected to the University's internal network via remote access technology, must use the most up-to-date anti-virus software; this includes personal computers.

7. Third party connections must comply with requirements as stated in the Third Party Agreement.
8. Personal equipment used to connect to the network must meet the requirements of University-owned equipment for remote access.
9. Direct network connections with outside organizations must be approved. The establishment of a direct connection between the University's systems and computers at external organizations, via the Internet or any other public network, is prohibited unless this connection has first been approved by the Dillard University IT Department and/or MYIT.
10. Inventory of connections to external networks must be maintained.

ANTIVIRUS/MALWARE/SPYWARE (Kaspersky) and Crowd Strike Falcon Cyber security cloud, DUO Security Agent:

1. All Servers, Desktop, Laptops, IPads, Tablets MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system.
2. All Faculty/Staff computer devices must have the Crowd Strike Falcon and DUO Security agent installed before accessing the network.
3. Enforcing and implementing this policy is to all IT operational staff at Dillard University. Responsibility for ensuring that new and existing systems remain in compliance with this policy resides with the Dillard University Desktop Support Manager. Any employee, student, faculty, guest, or contractors found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

J. Equipment Outsourced to External Service Providers
   1. The responsibility for the security of the equipment deployed by external service providers are to be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

K. Network Management/ Access Requirements
   1. All networks on the Dillard University campus will be install and maintained by the network manager and the Purple Guys Technology Services.
   2. To assure the integrity and availability of network services, no other network communications (with the exception of commercial cellular telephony networks) shall be permitted on University facilities
   3. No networking equipment (routers, managed switches, DHCP servers, DNS servers, WINS servers, VPN servers, remote access dial-in servers/RADIUS, wireless access points, hardware firewalls shall be permitted without a written exception from the Network Manager and MYIT Technology Services
   4. All devices starting January 1, 2023 are required to connect to the Dillard University network is register with Cisco Clear Pass appliance when initially attached to the network. This applies to printers, computing systems, laboratory equipment, and communications devices that use TCP/IP network protocols. The registrant must be a current faculty, staff, student, or affiliate account user with a valid and active Network ID. Information on how to register a network device can be obtaining by contacting the ITT Help Desk. Unregistered devices are subject to disconnection from the DU Network, without notice, whether or not they are disrupting network service.
   5. Currently devices connected to the DU Guest (DU-Visitors) wireless network are unregistered. As wireless registration services become available, all university-purchased or owned hosts shall be register in a similar manner to wired network registration. HU users accessing the Dillard's IT resources via wireless networking may assure the privacy of the network communications by using the DU VPN software.

8. **SECURITY**.

8.1 Security Measures. Jenzabar represents that it has and will maintain administrative, physical, and technical safeguards designed to: (i) protect against anticipated threats or hazards to the security of Confidential Information or electronic student records, and (ii) protect against unauthorized access to or use of Confidential Information or electronic student records. Jenzabar's technical safeguards include firewalls, virus and intrusion detection, and authentication protocols. In order to continually improve its safeguards, Jenzabar reserves the right to make changes to the physical and technical safeguards, policies, and data security programs at any time, provided that Jenzabar will, at all times, maintain commercially reasonable information security procedures and standards. The Client commits to take commercially reasonable security precautions to prevent unauthorized or fraudulent use of Confidential Information and/or electronic student records. Upon request, but no more than once per year, the Client may obtain a copy of Jenzabar's or its provider's most recent third party security audit summary report for applicable Jenzabar services. To the extent that Jenzabar is providing the Cloud Services itself, Jenzabar has implemented commercially reasonable, written policies and procedures addressing potential security breaches and haves a breach response plan in place.

8.2 Notice of Security Breaches. Within forty-eight (48) hours of discovery, Jenzabar shall report any Security Breach to the Client. For the purposes of this Addendum, a "Security Breach" means any unauthorized access, use, disclosure, modification, or destruction affecting the confidentiality of the Client's Confidential Information or electronic student records. Security Breaches shall not include: (i) "pings" on an information system firewall; (ii) port scans; (iii) denial-of-service attacks that do not result in a server being taken offline; or (iv) malware (e.g., a worm or virus) that does not result in unauthorized access, use, disclosure, modification, or destruction of the Client's Confidential Information or electronic student records.

8.3 Duties in the Event of a Security Breach. In the event of a Security Breach due to a lack of controls for which Jenzabar is responsible, Jenzabar will use commercially reasonable efforts to mitigate any negative consequences resulting directly from the Security Breach and will use commercially reasonable efforts to implement procedures to prevent the recurrence of a similar Security Breach. In the event of a Security Breach due to a lack of controls for which the Client is responsible, the Client will use commercially reasonable efforts to mitigate any negative consequences resulting directly from the Security Breach and will use commercially reasonable efforts to implement procedures to prevent the recurrence of a similar Security Breach, in which case Jenzabar agrees to provide assistance for a separate fee.

8.4 **Destruction.** At the conclusion of the provision of Cloud Services, Jenzabar or its provider shall use industry standard methods for the destruction of the Client's Confidential Information and electronic student records.

Wireless Access Policy

Overview

Wireless technology provides a convenient mechanism for accessing the university resources. These technologies have become ever-present in our workplace environment. The advent of wireless technologies adds increased functionality but also adds security risks and concerns that must be managed and mitigated.

Purpose

This policy provides a set of procedures and standards for implementing wireless technologies within the Dillard University network environment. It provides network administrators who deploy and manage wireless technologies with a baseline set of requirements that document connectivity, security, and device oversight.

Scope

This policy applies to all Staff and Outsource Vendors who engineer, install, or support the university wireless networks.

Policy

By using wireless devices within the Dillard University network for access purposes, all faculty, staff and students are subject to policies managing their use. All wireless devices including personal computers/laptops, smartphones, tablets, TV's or other devices are subject to the guidelines and procedures set forth in this policy.

CONNECTIVITY CONSIDERATIONS

Wireless networks are comparatively limited in speed, bandwidth, and coverage to wired networks. Where possible, the use of a wired connection is preferred because it is faster and does not compete with other wireless devices for bandwidth. However, use of wireless devices is increasing as it provides a convenient mechanism for accessing resources. Along with this convenience is a need for managed security as the devices are natively less secure than a hardwired device. The following procedures and practices shall be implemented to reduce risks related to wireless networks:

- Wireless networks shall be segmented between external guest and internal networks. Non-University devices shall not be connected to the Dillard University internal network
- Users inside the university firewall shall not connect to the internal network if they are using a bridged wireless connection to connect to an external network
- Wireless access points or routing devices with wireless capability are not allowed unless approved by the Information Technology Department.
- Logical and physical user access to wireless network devices shall be restricted to authorized personnel and devices excepting for access to a guest network

- Perimeter firewalls shall be implemented and configured by support staff to restrict unauthorized access and traffic metering
- All vendor default settings for wireless devices (e.g. passwords, wireless encryption keys, SNMP community strings) shall be changed prior to installing wireless equipment in a production environment
- Wireless security protocols shall be used that are of the highest encryption possible
- Strong passwords shall be employed for all wireless SSID and changed on a periodic basis either through the protocol or across the enterprise
- Ad-hoc wireless device audits shall be conducted on at least a quarterly basis to determine if any rogue devices exist on the university network
- Findings shall be presented immediately to the Network Manager and all rogue devices will be removed from the network

SECURITY

Wireless (Wi-Fi) transmissions used to access Dillard University networks and devices shall be encrypted. If sent across a public or open network, both the authentication data (e.g. a user ID and password) and the data itself shall be encrypted with strong encryption. Data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission security protocols along with approved encryption techniques are utilized.

The University Information Technology Department or a designee shall ensure:

- Sensitive information is encrypted using the strongest and most cost effective encryption available
- Wireless networks transmitting sensitive information or connected to sensitive information environments, use industry best practices to implement strong encryption for authentication and transmission
- Processes test for the presence of rogue wireless access points and detect and identify all authorized and unauthorized wireless access points
- Procedures maintain an inventory of authorized wireless access points including a documented business justification
- Response procedures exist and are implemented in the event unauthorized wireless access points are detected
- Older encryption protocols such as Wired Equivalent Privacy (WEP) or SSL are not used for authentication or transmission

Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the university. Satisfactory examples of evidence and compliance include:

- Spot user checks for compliance with this policy
- Archival documentation of quarterly checks and any remediation required
- Anecdotal communication evidence of policy implementation via email, logs, or other documentation

Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

Distribution

This policy is to be distributed to all faculty, staff, students, and contractors using Dillard University information resources.

Policy Version History

Version	Date	Description	Approved By
1.0	**6/1/2022**	**Initial Policy Drafted**	

WI-FI Usage at Dillard University

Your Wi-Fi devices can interfere with others' Wi-Fi connectivity.

- Wi-Fi networks use a range of publicly available, unlicensed radio frequencies shared among numerous types of devices.
- When many devices use these same frequencies, it can degrade Wi-Fi network performance.
- Many devices have an impact — wireless printers, microwave ovens, cordless phones, wireless audio speakers, wireless clocks, projectors, cameras, and gaming controllers.

Wired connection

- Always faster than Wi-Fi.
- Helps free up Wi-Fi for other users.

Reduce Wi-Fi interference.

Avoid using any device that can create a personal wireless network.

This type of ad hoc network created by individual devices, which can communicate directly with each other without using a router.

Example: For a **wireless printer**, disable its wireless capability and use a wired connection instead.
NOTE: The most common source of Wi-Fi interference are wireless printers creating ad hoc networks.

Avoid using a personal Wi-Fi router or access point.

These devices significantly interfere with the campus Wi-Fi network.

If you believe that your situation requires a personal access point, please request assistance from the IT Department.

Minimize interference from your other devices.

Know your personal impact on Wi-Fi.

The following table lists devices commonly used on campus and their impacts on Wi-Fi at various ranges. It also suggests solutions you can implement to reduce your impact.

Device	Impact	Range	Suggested Solution
Microwave oven	Very Severe	Short	Keep microwave away from wireless devices.
Wireless router	Very Severe	Very Long	Avoid using personal router.
Wireless camera & projector	Severe	Very Long	Disable wireless. Use wired connection. For classrooms, contact your local IT support
Apple Time Capsule **Use only for data backup.**	Severe	Very Long	Disable wireless. Connect with Ethernet cable.
Wireless media player **e.g., Apple TV, Roku, Chromecast**	Severe	Long	Connect with cable if possible. Disable wireless unless connecting via Dillard University Wi-Fi.
Wireless printer	Severe	Medium	Disable wireless. Connect with cable. **NOTE: The most common source of Wi-Fi interference is wireless printers creating ad hoc networks.**
Wireless speaker	Severe	Medium	Use wired speaker.
Wireless gaming controller	Severe	Short	Power off when not in use.
Cordless phone	Severe	Short	Do not use 2.4 GHz or 5 GHz cordless phones.
Bluetooth device	Medium	Short	Power off when not in use.
Certain computer displays	Medium	Short	Power off when not in use.

OUTDOOR WIFI CAMPUS MAP

HP Aruba 577 Outdoor Wireless Access Points

Spaces marked in orange are outdoor WIFI coverage areas.

- Back of Rosenwald Hall
- Back of Stern Hall
- Front of Alumni House
- Front of Straight Hall
- Between Hartzell Hall and Library
- Front of Kearny Hall (Avenue of the Oaks)
- Back of Kearny Kabacof Plaza
- Front of Dent Hall
- East of Dent Hall Parking Lot
- Back of Chapel and Gentilly Gardens Parking Lot
- Gentilly Gardens Court Yard A (Apt. 3500-3538)
- Gentilly Gardens Court Yard B (Apt. 3540-3598)
- Gentilly Gardens Court Yard C (Apt. 3604-3642)

MAP LEGEND

1. LAWLESS MEMORIAL CHAPEL
2. ROSENWALD HALL
3. STERN HALL
4. COOK FINE ARTS
5. CENTRAL PLANT BUILDING
6. ALUMNI HOUSE & WELCOME CENTER
7. HOWARD HOUSE
8. STRAIGHT HALL
9. OLD POWERHOUSE
10. HENSON HALL
11. WILLIAMS HALL
12. KEARNY HALL
13. CAMPHOR HALL
14. HARTZELL HALL
15. ALEXANDER LIBRARY
16. CAMPUS POLICE STATION
17. GENTILLY GARDENS APARTMENTS
18. MICHAEL AND SHAUN JONES HALL
19. DENT HALL
20. TENNIS CENTER
21. LAWLESS GATES
22. DUCK POND
23. KELLER AVENUE OF THE OAKS
24. PROFESSIONAL SCHOOLS AND SCIENCES BLDG.
25. STUDENT UNION, RECREATION, HEALTH & WELLNESS CENTER

DU ITT Procedures

Services Provided by ITT

- Email Accounts hosted by Gmail.
- Internet Access hosted by Cox Communications
- Network Login Accounts via Active Directory Services
- Microsoft Office 365
- Desktop & Laptop Support for Windows Machines
- Cox Cable Television Services
- Avaya Phone Services
- Audio visual setups during hours of 8:00a.m.- 4p.m. Monday- Friday
- Jenzabar Administrative Access

DU New Employee

Account Creation

All employee account creations generated when HR fills out The New Employee Google Form **https://goo.gl/forms/k51cg8cZC2py9zEb2**. When the form is filled out, ITT will contact listed supervisor to see if a machine and phone is already located in the Office. All account information is sent to the new employee's personal email provided to ITT by HR in the New Employee Form one business day before the new employee's start date.

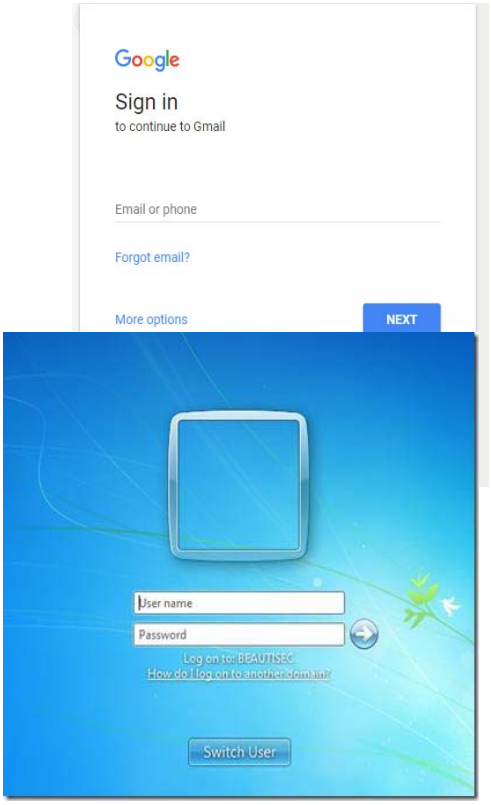
DU Email Account

General Information

All Dillard University email accounts are hosted by Gmail and is to be utilized by navigating to **www.gmail.com**. Hosting out email accounts allows all users' students included access to the Google suite. A set of intelligent apps including Gmail, Docs, Drive and Calendar that you can access, no matter where you are in the world. Student Email accounts are created once cleared with admissions and information is communicated during SOAR. While Faculty & Staff email accounts are created when HR submits a New Employee google form. Once from HR account information is communicated via personal email address provided by HR.

Access Information Students

The Login address is: **https://www.gmail.com**



Email Address is your FirstName.LastName@Dillard.edu

Password is configured like this: the first two letters, in lowercase, of your first name followed by your DU ID#

For the safety of our network we require all accounts be enrolled into **2 Step Verification**. If you have not enrolled your account, it will be automatically locked out. Please visit Howard House so ITT can assist you with enrolling.

Access Information Faculty & Staff

Email Address is your FirstIntial and LastName@Dillard.edu (possible middle initial for users who have common Last Names)

Password is configured like this: the first two letters, in lowercase, of your first name followed by your DU EMPLOYEE ID#
For the safety of our network we require all accounts be enrolled into **2 Step Verification**. If you have not enrolled your account, it will be automatically locked out. Please visit Howard House so ITT can assist you with enrolling.

Two Step Verification

Two-step verification is a second layer of security required on all email accounts. If your password is ever hacked, it will protect your account from being accessed, as the hacker will not have access to your cell phone where your verification code is being sent too. This extra layer of security protects our entire domain from spamming, phishing, and putting both students and employees' information at risk. If you switch cell phones and need the number update for two-step verification, please contact ITT before attempting to do so on your own.

DU Network Login

Network Access Security Information

Individuals may use Dillard University computing facilities only with the express authority of Dillard University. The administration at Dillard University authorizes system accounts and access, and reserves the right to monitor and/or audit any system belonging to the university at any time. Using an account that belongs to another individual or giving an individual other than the owner access to any Dillard University account is strictly prohibited. Each User is legally responsible for all activity originating from his or her account.

Access Information (Student)

All student accounts are created before the start of the semester when cleared with Admissions. Information is communicated via SOAR sessions that all new students are required to attend. If for some reason a student does not receive his or her information they can come to Howard House and receive the information or simply email **helpdesk@dillard.edu**

Username: Will be your email address
Example: Dana.Williams@Dillard.edu

Password is configured like this: the first two letters, in lowercase, of your first name followed by your DU ID#

Access Information (Employees)

All Faculty & Staff email accounts are created when HR submits a New Employee google form. Once from HR account information is communicated via personal email address provided by HR.

Username: Will be your email address
Example: DWilliams@Dillard.edu

Password is configured like this: the first two letters, in lowercase, of your first name followed by your DU EMPLOYEE ID#

ITT HELPDESK

Submitting Help Desk Request

All requests for ITT support should be submitted to **helpdesk@dillard.edu** . The importance of submitting a ticket through the proper channels allows ITT to properly prioritize their workload and also allows open communication with ITT via the Ticket number. Once the ticket is assigned you will receive either a follow up phone call or email from the assigned tech. If your machine is completely down, please call 504.816.4716 & report outage to Switchboard Operator who will then make sure the proper party in ITT is informed of said incident.

Microsoft Office 365

Accessing Office 365 for free

Microsoft Office 365 is available to all students, faculty, and staff with valid Dillard University Email Accounts. To install the Office Suite on non-Dillard machines please use the following link: **https://products.office.com/en-us/student/office-in-education**

Campus Wi-Fi

Access for Employees

To access the Wi-Fi **(DUEMP)** via your smartphone, laptop, tablet or other personal devices continue using your existing Username and password. If you are unable to connect to **DUEMP,** please see ITT for assistance and/or Wi-Fi Access Manual

Username is {***first initial of your first name plus your entire last name***}
Example:
Username: tlucien
Password: ti123456

Access for Students

To access the Wi-Fi **(DUSTUDENTS)** via your smartphone, laptop, tablet or other personal devices continue using your existing Username and password. If you are unable to connect to **DUSTUDENTS,** please see ITT for assistance and/or Wi-Fi Access Manual

Username is {***first name.last name***}
Example:
Username: tia.lucien
Password: ti123456

Access for Smart TV, Xbox, Playstation, etc.

To access the network thru these devices you will need to manually add the hidden network name that is **dusmart or dusmart2** {all lowercase} The password is **du26011869**

Audio Visual Setup Request

Submitting Request for A/V

All requests for Audio Visual needs between the hours of 8:00a.m.-4:00p.m. Monday- Friday need to be submitted at least 3 days prior to event. The request needs to be sent to helpdesk@dillard.edu. Once the request is received ITT will contact you to confirm setup date, time, location, & equipment needed. If the request for A/V needs are not submitted properly ITT cannot guarantee the setup or equipment needed for said event.

Cable TV Services

Submitting Request for Cable TV

Cable Television Services are provided to all residential housing units & selected common and office areas throughout the campus. Channel selections include all local & basic cable channels.
All requests for service and repairs should be submitted via email to **helpdesk@dillard.edu** please include contact information and exact location of the service.

Jenzabar Account Access

Requesting Jenzabar Account

To request the creation of an employee's Jenzabar account please submit a ticket via **helpdesk@dillard.edu**. Once a ticket is created, you will receive an email with the Jenzabar Access Form attached. The form must be completed and signed by all necessary parties. Each department is responsible for training employee on their module before Jenzabar account access is given. Please do not request account until said training is completed.