SUBJECT: Information Technology Services (ITS)	REFERENCE:
	PAGE: 1
UNIVERSITY OF HOLY CROSS	OF: 19
	EFFECTIVE:
APPROVED BY David M. Landry	REVISED: 2/2/2017

FORWARD

The ability of the University of Holy Cross to deliver services to the faculty, administration, staff, and students has grown enormously through the use of computers. The University of Holy Cross has made significant investments in information resources and plans to continue to invest. While the value of equipment such as computer hardware is easily appreciated, we must not overlook the larger investment in less tangible information assets – such as data, software, and automated processes.

Information resources are vital assets, which require protection. Data, whether stored in central computers accessible through remote terminals, processed locally on microcomputers, or generated by word processing systems and other software products, are vulnerable to a variety of threats and must be afforded adequate safeguards.

The University of Holy Cross faculty, administration, staff, and students need to be aware of the value of these resources and the means of protecting them. User awareness through education is the first line of defense in maintaining confidentiality, reliability, availability, and integrity of the University of Holy Cross University information resources.

The University of Holy Cross Technology Policy was developed to provide guidelines for faculty, administration, staff, and students in the need for and means of protecting the University of Holy Cross information resources. This document defines the security and data ownership responsibilities of the mission critical computing resources, academic and administrative, which are maintained and operated by the University of Holy Cross Information Technology Services. This document should be useful in ongoing departmental security programs for security awareness and training.

INTRODUCTION

Continuing availability of information is essential to the operation of the University of Holy Cross programs. Expanded use of computers and telecommunications has resulted in more accurate, reliable, and faster information processing, with information more readily available to administration, faculty, staff, and students, than ever before. The University of Holy Cross will realize increased productivity, in terms of improved delivery of services, enhanced administrative capabilities, and lower operating costs, as a direct result of the growing commitment to use information technology.

Information technology has also brought new administration concerns, challenges, and responsibilities. Information assets must be protected from natural and human hazards. Policies and practices must be established to ensure that hazards are eliminated or their effects minimized.

The focus of information security is on ensuring protection of information and continuation of program operations. Providing efficient access to necessary information is the impetus for establishing and maintaining automated information systems. Protecting that information and the surrounding investment is the reason for establishing an information security program.

Protecting information assets includes:

- Physical protection of information processing facilities and equipment. Maintenance of applications and data integrity.
- Assurance that automated information systems perform their critical functions correctly, in a timely manner, and under adequate controls.
- Protection against unauthorized disclosure of information.
- Assurance of the continued availability of reliable and critical information.

Many program operations that were traditionally manual or partially automated are today fully dependent upon the availability of automated information services to perform and support their daily function. The interruptions, disruption, or loss of information support services may adversely affect the University of Holy Cross's image and ability to administer programs and provide services. The effects of such risks must be eliminated or minimized.

Additionally, information entered, processed, stored, generated, or disseminated by automated information systems must be protected from internal data or programming errors and from misuse by individuals inside or outside the University of Holy Cross. Specifically, the information must be protected from unauthorized or accidental modification, destruction, or disclosure. Otherwise, we risk compromising the integrity of the University of Holy Cross programs, violating individual rights to privacy, violating copyrights, or facing criminal penalties.

An effective and efficient security management program requires active support and ongoing participation from multiple disciplines and all levels of administration. Responsibilities include identifying vulnerabilities that may affect information assets and implementing cost-effective security practices to minimize or eliminate the effects of the vulnerabilities.

The Policies and procedures of this document apply to the mission critical applications and resources operated by the University of Holy Cross ITS department. These include applications such as PowerCampus, PowerFAIDS, Great-Plains, and Microsoft Office; the campus computer network; and the computing facilities such as the administrative server(s) environment with Windows 2008, Microsoft SQL 2008, and all microcomputers with Windows OS.

In the remainder of this document information resources will refer to:

- Network Resources – the UHC computer network.
- Hardware Resources – all computing resources operated by ITS.
- Software Resources – all mission critical applications operated by ITS

In the remainder of this document ITS will refer to the Information Technology Services Department; supervised by the Director of Information Technology.

GENERAL POLICY

It is the policy of the University of Holy Cross that:

- Information resources are valuable assets and unauthorized use, alteration, destruction, or disclosure are not allowed. Attempting to circumvent security, administrative access controls, or hardware/software policy for Information resources is a violation of this policy. Assisting someone else or requesting someone else to circumvent security or administrative access controls is a violation of this policy. Information resources may be used only for official university purposes.
- Violations of the Computer Security Policy will be reported to ITS, the President and H.R. and will be subject to appropriate administrative action.
- All employees will receive the UHC Computer Security Policy. New employees will receive a copy of the statement at hire.
- User-ids and passwords must control access to all information resources except for those specific resources identified as having public access. Each user will be required to change their password according to the guidelines. The user-id owner is responsible for all actions and functions performed under their user-id.
- Information, which by law is confidential, must be protected from unauthorized access or modification.
- Data, which is essential to critical functions, must be protected from loss, contamination, or destruction.
- Confidential information shall be accessible only by personnel who are authorized, in writing, by the department supervisor. The performance of duties as it relates to this authorization is determined on a strict "need-to-know" basis. Data containing any confidential information shall be readily identifiable and treated as confidential in its entirety.

- An auditable, continuous chain of custody shall record the transfer of confidential information. When confidential information from a department is received by another department in the connection with the transaction of UHC business, the receiving department shall maintain the confidentiality of the information in accordance with the conditions imposed by the providing department.
- All employees accessing a mission critical administrative application must receive appropriate training for using the application and must acknowledge the security and privacy requirements for the data contained in the application.
- When an employee terminates employment, H.R. will notify ITS to terminate their access to information resources. Similarly, students who are not enrolled will have their access to information resources terminated.
- All information resources used for mission critical applications shall have a cost effective, written contingency plan that will provide for prompt and effective continuation of critical missions in the event of a disaster.
- Microcomputer end-user workstations used in sensitive or critical tasks must have adequate controls to provide continued confidentiality, integrity, and availability of data stored on the system. End-users must not leave their workstations unattended while it is logged on.
- All microcomputer end-user workstations should have virus protection software installed.
- Computer software and hardware purchased using University, grants, donations or federal or state funds is UHC property and shall be protected as such. Therefore, it is completely subject to all policies therein with no exceptions.
- Administrative rights to computers is reserved for ITS personnel only.
- Internet access to the UHC Network will be controlled as appropriate under guidelines established by the Director of Information Technology.
- ITS is responsible for all technical aspects of computer hardware and software. The purchase of campus wide software applications is to be reviewed by the Academic and Administrative Computing Committee.
- Updates will be pushed to desktop computers on the Friday after the 15th of each month. Users are responsible for ensuring that all work is saved before leaving at the end of the work day on these days.
- To ensure the integrity and functionality of our network environment, server updates will be conducted on the Friday after the 15th of each month during non-working hours.

EMAIL POLICY

The University of Holy Cross provides all administrators, faculty, staff, and students of the University with a university e-mail account. This account is to be used by members of the University community for all University-related communication between personnel, students, and/or outside individuals or organizations. The University e-mail system provides a means of communication which is secure, efficient, reliable, and easily accessible through the World Wide Web.

The University e-mail system is to be used by all administrators, faculty, staff, and students as the official means of communication. All official e-mail correspondence from the University is to be sent through the University's e-mail system. No University personnel are to require e-mail correspondence to be sent to or received from an e-mail service other than the University's. Students may retain their UHCNO.edu email account as long as they are actively enrolled. Alumni may retain access to their UHCNO.edu email account as long as they are actively using it. Alumni accounts that have not been accessed within 180 days will be removed from the system.

Assignment of Student E-MAIL

ITS will assign each student an official UHC e-mail address at the time of first enrollment. All student e-mail accounts are password-protected. The privacy and security of e-mail accounts depends on the appropriate use and protection of user IDs and passwords. Students should not share their username and password with anyone. This e-mail address will be in effect during the student's academic career.

Sending Mass E-Mails

UHC email accounts should not be used to send mass emails to non UHC email accounts. Mass emails could result in University wide blackballing from other organizations. Mass email campaigns should only be sent through mass communication email service providers.

Dean or Supervisor approval is required for permission to send mass emails to all faculty, staff, or students.

AUDITOR ACCESS

There will be occasions when auditors require access to information resources and data files. The access will be permitted according to these guidelines:

Auditors and Consultants:

Auditors and Consultants will be granted access to information resources and data files on an as needed basis after coordination with the Department heads and data owners, and after proper training requirements are met.

TERMS AND DEFINITIONS

The following terms used in this document are defined to have these meanings:

PowerCampus	The administrative application for processing students through all aspects of their University careers. This program encompasses Admissions, Billing, Registrar/Academic Affairs, Institutional Advancement and Information Technology
Grcat Plains	Thc administrative application for accounting for the University.
Computer Security	Those measures, procedures, or controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure, modification, or destruction.
Data	A representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means.
General Accessible Computing Resource	The computing resources of the University of Holy Cross available to any faculty, staff, or student at UHC.
Information Resources	The computer hardware, software, data files, and networks at UHC.
LAN	Local Area Networks are connected to the UHC network and are departmental resources.
Mission Critical Information Resources	Those information processing resources that have been determined to be essential to UHC's critical missions and functions.
UHC Network	The Ethernet, Fiber optic, and the port selector portions of the UHC campus computing nctworks.
Password	A combination of characters used to authenticate a person's identity to a computer system when associated with a user-id.
PowerFAIDS	The administrative application for processing student Financial Aid information.
User-Id	A unique identifier used by the computer system to establish user identification.
CollegeBoard	The administrative application used for transmitting student Financial Aid information to the Federal Government.
Cisco VOIP	Voice over Internet Protocol – The Campus telephony system now uses all data drops/outlets for voice communication, in addition to data transfer. Much more efficient use of infrastructure and ease of expansion as there is no further need for phone lines to be installed or used. Only fax lines are still analog/RJ11.
POE	Power Over Ethernet- Our campus data lines and switches are POE now, which allows power injection for wireless points and Cisco IP telephones. Eliminates need for further electrical installations/lessens power use.

PASSWORD POLICY

Information handled by computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. Effective controls for logical access to information resources minimize inadvertent employee error and negligence, and reduce opportunities for computer crime. Each user of a mission critical automated system is assigned a unique personal identifier for user identification. User identification is authenticated before the system may grant access to automated information.

Password Selection

Passwords are used to authenticate a user's identity and to establish accountability. A password that is easily guessed is a bad password which compromises security and accountability of actions taken by the user-id which represents the user's identity.

Today, computer hackers are extremely sophisticated. Instead of typing each password by hand, hackers use personal computers to try to guess the passwords, automatically retrying when they become disconnected. Instead of trying every combination of letters, starting with AAAAAA (for example), hackers use hit lists of common passwords such as WIZARD or DEMO. Even a modest home computer with a good password guessing program and a broadband internet connection can try thousands of passwords in less than a day's time. Hit lists used by hackers may contain several million words. Therefore, any password that anybody might guess to be a password is a bad choice.

What are popular passwords? Your name, your spouse's name, or your parents' names. Other bad passwords are these names spelled backwards or followed by a single digit. Short passwords are also bad, because there are fewer characters; they are more easily guessed. Especially bad are "magic words" from computer games, such as XYZZY. Other bad choices include phone numbers, characters from favorite movies or books, local landmark names, favorite drinks, or famous people.

Some rules for choosing a good password are:

- Use both uppercase and lowercase letters in random combinations.
- Choose something easily remembered so it doesn't have to be written down.
- Use at least 6 characters. Remember, the password must contain *at least* one capital letter *and* one number or special character.
- It should be easy to type quickly so someone cannot follow what was typed by watching the keyboard.

Password Handling

A standard admonishment is "never write down a password." You should not write your password on your desk calendar, or a post-It label attached to your computer terminal, or on the pull-out drawer of your desk.

A password you memorize is more secure than the same password written down, simply because there is less opportunity for other people to learn a memorized password. But a password that must be written down in order to be remembered is quite likely a password that is not going to be guessed easily. If you store a password in your wallet, the chances of somebody stealing your wallet using the password to break into your computer account are remote.

If you must write down a password, follow a few precautions:

- Do not identify the password as being a password.
- Do not include the name of the account or the phone number of the computer on the same piece of paper.
- Do not attach the password to a terminal, keyboard, or any part of a computer.
- Mix in some "noise" characters or scramble the written version of the password in a way that you remember, but make the written version different from the real password.
- Never record a password on-line and never send a password to another person via electronic mail.

ITS DISASTER RECOVERY

As a University, UHC has become heavily reliant on Information Technology for its day to day operations. The IT infrastructure now plays an important role in the daily administration of the University in the areas of teaching, communication, and administration. It is an integral part of the way UHC does business.

Listed below are the crucial systems that would need to be restored in the case of a disaster. Depending on the incident response and assessment, the Disaster Recovery Team would have to assure integrity/ recovery of systems in order of priority.

- Network infrastructure / Switches
- NAS, Unitrends, Storevault
- Domain Controllers (ScanServ, DC1, DC2, UHC)
- VSP-1, VSP-2, VSP-3, VM1, VM2, King, Queen, Jack Chaos, RS-Proteus, Call Managers

- Watchman, VP12012, Muses, WDS, DirSync, kms-HOST, Targetx, Keyscan08
- Desktop Recovery (Faculty, Staff, and Labs), ASC-2, ASC-NCOM, Destiny
- Classroom Technology Recovery

Depending on the magnitude of the disaster, departments, divisions, or offices may have to accommodate for any changes in performance and operation. In addition, the campus community may have to make allowances for any relocations to get access to equipment for daily operations.

This plan may be modified or substantial deviations thereof may be required in the event of unusual or unforeseen circumstances.

ITS Disaster Recovery Team

Information Technology Services personnel will make up the ITS/DRT. Roles and functions will be defined in the following section. The ITS/DRT will work closely with members of the UHC Disaster Recovery Team to coordinate efforts in the recovery process.

Responsibilities of Each Team Member

The Director of ITS will initiate the incident response followed by an assessment and disaster declaration. In close collaboration with the UHC Disaster Recovery Team, the Director will coordinate efforts to put into effect the recovery plan with the ITS and will work along with the Campus Technology Technician to restore all network and communication services.

The ITS Help Desk Coordinator(s) will coordinate the recovery plan working with the Director of ITS. As part of the initial incident response, the Coordinator(s) will make sure that all the appropriate staff members are contacted and debriefed regarding procedure depending on the damage assessment. The Coordinator(s) will be responsible for supporting students and faculty in classrooms and the Academic Skills Center.

The Campus Technology Technician will restore network and communication services.

The Senior Database Administrator (SDBA) will be responsible for restoring Power Campus, Chaos, Self-Service, and PowerFaids.

The Web Services Coordinator will be responsible for all information updates, updating all web page notices, Blackboard-connect, mass emails and social media. Coordinator will provide Self Service support and web support for UHC public pages.

The ITS Help Desk Coordinator(s) will be responsible for testing all systems from the perspective of a user to ensure that all systems are running as expected. The technician will respond to all help desk calls from faculty, staff and students.

Disaster Preparedness

Regularly scheduled backups of all mission-critical systems on campus will be standard procedure (see list above). ITS will routinely backup offsite using the cloud services vendor.

Disaster Recovery and Procedures

- Incident response
- Assessment and disaster declaration
- Incident planning and recovery
- Post incident review

Backup Strategy and Retention

Daily and weekly backups will be sent to the cloud services vendor in the event of a prolonged disaster. Critical applications will be temporarily restored in the cloud.

Recovery Priority List

- Network infrastructure / Switches
- NAS, Unitrends, Storevault
- Domain Controllers (ScanServ, DC1, DC2, UHC1)
- VSP-1, VSP-2, VSP-3, VM1, VM2, King, Queen, Jack Chaos, RS-Proteus, Call Managers
- Watchman, VP12012, Muses, WDS, DirSync, kms-HOST, Targetx, Keyscan08
- Desktop Recovery (Faculty, Staff, and Labs), ASC-2, ASC-NCOM, Destiny
- Classroom Technology Recovery

PERSONNEL SECURITY AND SECURITY AWARENESS

The mission of ITS is to support the mission of the University by ensuring the integrity of data, protecting confidentiality, and securing equipment and systems. To ensure the integrity of the network administrative access is reserved for ITS personnel or consultants. System updates and software installations should be installed by ITS personnel only.

Information assets addressed by the policy include data, information systems, computers, and network devices.

The University will:

- Establish a security framework to appropriately secure access to information resources and services.
- Protect against unauthorized access confidential information.
- Protect against threats or hazards to the security of information assets
- Comply with federal, state, and local law, University policies, and agreements

EMPLOYEE REQUIREMENTS

University President, Vice Presidents, Deans, Directors, Chairs, Supervisors are responsible for implementing and ensuring compliance with this policy. Responsibilities include:

- Communicating this policy within their department
- Providing security and awareness training within their department
- Ensuring the implementation of information security within their department

The Information Technology Services is responsible for:

- Directing and coordinating the ITS Security Program;
- Determining compliance with this policy
- Assisting units in fulfilling their information security requirements.

Each member of the campus community is responsible for the security and protection of information resources in accordance with federal, state, and local law. The physical and logical integrity of network resources, must be protected from threats such as unauthorized access and damage. Employees are expected to maintain the security of confidential information as well as protect computer systems.

Acknowledgment of Rights and Responsibilities

Employees with access to administrative application systems acknowledge the security requirements of the systems and their responsibility to maintain the security of the systems before access to the system is granted. This acknowledgment occurs by signing the application statement of security responsibility during mandatory training sessions, and by presentation of an on-line statement when the application is accessed.

Hiring and Termination Procedures

UHC departments should take advantage of opportunities arising through hiring and termination of employees to reinforce security awareness and to train them regarding their obligations in UHC ITS security policies and procedures. Upon termination of an employee, H.R. will notify ITS to revoke all access authorizations to information resources.

Computer Security Rules, Regulations, and Laws

There are University regulations and a number of federal laws that affect the security of information processing resources, computers systems, computer software, and data files. The following summaries are provided for the reader to review:

Federal Copyright Law
Recognizes that all intellectual works are automatically covered by copyright. The owner of a copyright holds the exclusive right to reproduce and distribute the work.

Computer Fraud and Abuse Act of 1986
Makes it a crime to access a computer to obtain restricted information without authorization; to alter, damage, or destroy information on a government computer; and to traffic in passwords or similar information used to gain unauthorized access to a government computer.

Computer Application Development Controls

All ITS staff is required to adhere to the following security guidelines:

- Systems and programs must perform only the functions requested and may not cross over into other systems except as specified in the approved specifications.
- System development resources such as terminals, microcomputers, and development software will only be used for approved projects.
- Modifications must be approved by the development management and management of the organization that "owns" the application system.
- Unauthorized changes to production systems are not allowed and are considered violations of the UHC Computer Security Policy and computer security laws.
- Procedures are required which include adequate testing prior to implementation, security against modification of production data, controlled access to data, production, and program libraries.
- Security procedures, work practices, programming methods, standards, production libraries, and overall data security will be subject to review by the ITS staff and the Academic and Administration Computing Committee.

- Running of programs that update production databases should be done only by the ITS staff and not programmers.
- UHC administrative staff, faculty, and students should only have read-only access to production programs libraries and should not have access to program source code libraries.
- Movement of test programs into production program and source code libraries must be approved by appointed application administrators.
- All change requests and problem reports must be in written form and have the approval of authorized ITS personnel.
- All new database structures and changes to existing database structures must be approved by the Database System Administrator before the modified structures are put into production.
- Managers will ensure reviews are conducted on all new programs and changes to existing programs before the programs are moved into production libraries. Any exceptions must be reviewed and documented in timely manner.

COMPUTER SECURITY POLICY

The information resources at UHC are extensive and are readily available to authorized users. This availability of computer hardware, software, and database resources brings with it the responsibility to protect those resources from unauthorized access, unauthorized use, or inappropriate use. During the past several years, much has been written about viruses, worms, and hackers. While these are very real and present dangers, we must also be aware of the dancragers from careless activities regarding information resources at UHC, particularly in the network environment.

- Each user of an information resource must be responsible for certain key aspects of security, which include:
    - Appropriate handling of passwords and password procedures.
    - Using resources, hardware and software, in accordance with the vendor's guideline.
    - Taking precautions with regard to viruses.
    - Following the prescribed procedures for access and use of data.
    - Adhering to copyright policies.
- UHC has instituted certain computer security measures designed to protect the integrity of Information resources. Any attempt to circumvent these procedures may be a violation of UHC policies, rules, and regulations, and the state and federal statutes.
- All users of Information resources acknowledge their reading and understanding of computer security issues each time they logon to an UHC computer system.

HELP DESK POLICES

- Request for assistance with hardware and/or software must be submitted to the online helpdesk (Trackit) systems. ITS cannot honor request for assistance that have not been sent to the Trackit.
- Request for equipment setup, (example: laptops, projectors, speakers) must be made **one week** prior to the event. ITS cannot guarantee support for events that are not submitted within this time frame
- The help desk is open Monday – Thursday 8:30am – 7:30pm and Friday 8:30am to 5:00 pm. ITS will attempt to close all help desk tickets within 24-hours when possible. Weekend coverage is not available.
- Help desk tickets that require extended time to complete will be completed as soon as feasibly possible.
- Help desk tickets that are waiting for a response from the sender will be automatically closed if a response is not receive with two weeks.

PASSWORDS AND PRIVATE INFORMATION

The Help Desk has a responsibility to use our skills wisely and honestly, in a way that ensures the trust of our users and optimizes the health of the University, in accordance with the Password Policy and other policies.

- ITS never ask for passwords, period.
- ITS does not give out personal contact information. In some circumstances, we may directly contact a person on behalf of a client.

HARDWARE / SOFTWARE POLICY

The University is happy to provide computers for faculty, administration, staff, and students so that they can perform their work efficiently. These computers are the property of UHC and should be used in accordance with the following policies and procedures, as well as the Acceptable Use Policy outlined in the handbook. In order to consolidate licensing agreements, reduce demand for technology support, decrease the risk of licensing infractions, and track the University's technology resources, the University has adopted standardized hardware and software policies and procedures.

Policies and Procedures:

All computers on campus will be loaded with a "base install" of licensed software by the ITS department. The "base install" consists of:

- Microsoft Windows operating system
- Microsoft Office Suite
- Kaspersky Antivirus
- Adobe applications (Adobe Reader; Free Apps)
- Chrome and Internet Explorer

Hardware upgrades and software deemed necessary for the user's job function may be installed if requested through Track-It and subsequently approved by the appropriate supervisor. Requests for third-party software featuring functionality that already exists in "base install" programs are not guaranteed to be granted.

Hardware upgrades and software requests are subject to review in the following order: ITS Director, the user's immediate supervisor, Dean, and Vice Presidents.

Hardware upgrades and software requests must be made at least 15 working days prior to the date on which the hardware upgrades or software must be operational. ITS will coordinate with the users of these applications on upgrades to ensure proper timing and testing before going live.

The ITS Help Desk Coordinator will serve as the purchasing agent for all new hardware and software. Approved hardware upgrades or software requests will be purchased and installed by a member of the ITS staff. ITS will hold copies of all software and the appropriate licensing information after installation.

The University will not provide support for any hardware or software that was not purchased with University funds. ITS must receive the appropriate licensing information before they install software purchased by another department or individual. Please note that unauthorized installation of hardware / software violates University policy.

Transfer of documents on campus should be done in the default format for Microsoft Office programs, Adobe PDF, or Rich Text Format (RTF). Students cannot be required to submit documents to instructors in a format outside of the defaults for the "base install" programs.

Hardware upgrades and software requested through Track-It will be reviewed under the criteria below:

Requests will be granted if the requested materials provide a unique, job-essential function that is not provided by currently owned and licensed materials and if cost of obtaining the requested materials is not prohibitive.

Administrative access to campus computers is reserved for ITS staff only.

INTERNET USAGE POLICY

Internet access is available to students, faculty, staff and administrators to promote educational excellence at the University of Holy Cross by facilitating resource sharing, innovation, and communication.

1). Acceptable Use – Use of other organization's network or computing resources must comply with the rules appropriate for that network. Access and/or transmission of any material in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, unauthorized access to resources on any network or material protected by trade secret. Use of product advertisement or political lobbying is prohibited. Use for commercial or personal activities is not acceptable.

2). Privileges – The use of the Internet is a privilege, not a right, and inappropriate use will, at a minimum, result in cancellation of those privileges. The Director of Technology will assure that any reports of alleged violations are addressed through the appropriate channels.

3). Disclaimer - The University of Holy Cross makes no warranties of any kind, whether expressed or implied, for the service it is providing. The University of Holy Cross will not be responsible for any damages suffered. This includes, but is not limited to, loss of data resulting from delays, non-deliveries, viruses, missed-deliveries, or services interruptions caused by negligence error or omissions. Use of any information obtained via the Internet is at the users own risk. The University of Holy Cross is not responsible for the accuracy or quality of information obtained.

4). Security – Security on any computer system is a high priority, If users can identify a security problem on the UHC system, they must notify the Director of Technology. Identified problems must not be demonstrated to other users. Any user identified as a security risk or having a history of problems with other computer systems at a minimum, may be denied access to the Internet. All Internet transactions are recorded and can be traced to a particular username. For this reason, username and password must be kept secure; under no circumstance must another individual's account be used.

Users must LOGOUT after each initiated session.

- Users are responsible for what happens under their account; any security breach made under a user's account is his/her responsibility regardless of the circumstance.
- A user, having reason to believe that others may have obtained and could be using his/her username, must report it immediately.
- Users must make their password available to others or use any account set up for another user or make any attempt to find out the password of a facility or an account for which they do not have authorized access.
- Users must not under any circumstance, in messages or otherwise, represent themselves as someone else, fictional or real, without providing their real identity or username.
- Users must not access any data in the information technology facilities unless that data belongs to them or has been specifically and intentionally designated for public use or for the use of a group to which they belong.
- At any time and without prior notice, University administration reserves the right to examine e-mail, personal file directories, and other information stored on University computers and servers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of University information systems. (See the University of Holy Cross Technology Security Policy Manual).

5). Other forms of Unacceptable Use:

- Anything deemed illegal by Federal, State or local laws.
- Anything deemed academically dishonest.
- Unauthorized use of equipment or resources.
- Theft of equipment, software, and/or data.
- Harassment/Stalking.
- Willful impeding of networking traffic or hoarding of resources (equipment, software, and/or data).
- Misrepresentation of UHC or its entities.
- Use of UHC trademarks, logo, insignia or copyrights without prior approval.
- Access or proliferation of pirated software, offensive material or pornography.
- Executing unauthorized software applications.
- Installation of software without obtaining prior approval.
- Willful proliferation of computer viruses.
- Any action that would inhibit access to resources (such as implementing passwords of systems or applications) or restrict their use by other users.

6). Vandalism – Vandalism will result in disciplinary actions. Vandalism is defined as any malicious attempt to harm or destroy hardware, data of another user, Internet, or any agencies or other networks that are connected to the Internet. This includes, but is not limited to, the knowing or intentional uploading, creation, or dissemination of computer viruses.

7). E-Mail - The University of Holy Cross provides all administrators, faculty, staff, and students of the University with University e-mail account with the suffix - UHCNO.edu. This account is to be used by members of the University community for all University-related communication between personnel, students, and/or outside individuals or organizations. The University e-mail system provides a means of communication which is secure, efficient, reliable, and easily accessible through the World Wide Web.

The University e-mail system is to be used by all administrators, faculty, staff, and students as the default means of communication. All official e-mail correspondence from the University is to be sent through the University's e-mail system. No University personnel are to require e-mail correspondence with students to be sent to or received from an e-mail service other than the University's.

8). Terms and Conditions – All terms and conditions as stated in this document are applicable to all students and employees at the University of Holy Cross. These terms and conditions reflect the entire agreement of the parties and supersede all prior oral or written agreements and understandings of the parties.

PRIVACY POLICY

The University of Holy Cross cares about providing the faculty, staff and student body with information to manage and protect their Online privacy. This privacy policy outlines what information the UHC website collects, who may receive that information, and what UHC may do with the information.

The University of Holy Cross does not share, sell, or transfer personal information submitted via the web. Information involuntarily logged from the use of the University's website is for statistical purposes only. This type of information includes information such as the number of visits, the type of browser, or other technical means to view our web pages. This statistical information is not available for public viewing. In addition, every effort is made to use session cookies which do not store any information on your computer.

A person may voluntarily provide the University of Holy Cross with personal information via the website in a case where a user chooses to submit an Online form. Online forms may be submitted for reasons such as applying to the University of Holy Cross, requesting information, or other uses. Any information submitted via a form is not retained on the website.

The University of Holy Cross' Information Technology Services Department incorporates many security features for such as encryption, and secure logon for any page that a faculty, staff, student, or friend of the University logs into to view their personal information.

Some pages of University's website include links to external sites. Visitors should be aware that our privacy policy pertains only to the webpages of the University of Holy Cross.

For any additional information not covered in this policy, please contact the Information Technology Services Department at (504) 398-2106 or at trackit@uhcno.edu

I have read and understood this policy and will abide by all the articles herein:

Print Name

Signature

Date