Email Policy

1. Purpose

Thiel College currently utilizes three solutions for email; a College managed system located on College servers ("Exchange Accounts") and a cloud-based platform utilizing Microsoft's Office 365 ("Office 365 Accounts") using Thiel's Domain Name. Collectively these are known as "College Email Accounts."

The purpose of this policy is to ensure the proper use of each of those solutions.

Electronic Mail is a tool provided by the College and serves as a primary means of communication and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, ethical and lawful manner. Use of College Email Accounts evidences the user's agreement to be bound by this policy. In the event a College employee holds multiple College Email Accounts, the most stringent rules of this policy shall apply.

2. Policy Statement

2.1 Account Creation

College Email Accounts are created based on the official name of the staff or faculty member as reflected in Human Resource, Payroll or President's Office records. Student and alumni accounts are created based on user ID reflective of the name on file with the Registrar. Requests for name changes to correct a discrepancy between an email account name and official College records will be processed, in which case the email account name will be corrected. This could be due to error or a person legally changing their name. Requests for mail aliases based on name preference, middle name, etc., are evaluated on a case-by-case basis.

Faculty, staff, or departments can request temporary email privileges for users outside of the College. Full time Faculty or Staff requesting these types of accounts will be required to submit user information, rationale for account, expiration date, & sponsor information. Such requests shall be approved by the appropriate Director level manager.

2.2 Ownership of Email Data

The College owns all College Email Accounts. Subject to underlying copyright and other intellectual property rights under applicable laws and College policies, the College also owns data transmitted or stored using the College Email Accounts.

2.3 Privacy and Right of College Access

While the College will make every attempt to keep email messages secure, privacy is not guaranteed and users should have no general expectation of privacy in email messages sent through College Email Accounts. Under certain circumstances, it may be necessary for IT staff or other appropriate College officials to access College Email Accounts. These circumstances may include, but are not limited to, maintaining the system, investigating security or abuse incidents or investigating violations of this or other College policies, and, in the case of Gmail/Office 365

Accounts, violations of Google's or Microsoft's Acceptable Use Policy or the College's contracts with Google and Microsoft. IT staff or College officials may also require access to a College Email Account in order to continue College business where the College Email Account holder will not or can no longer access the College Email Account for any reason (such as death, disability, illness or separation from the College for a period of time or permanently). Such access will be on an as-needed basis and any email accessed will only be disclosed to individuals who have been properly authorized and have an appropriate need to know or as required by law.

All email users are bound by the appropriate acceptable use policy of both Thiel College and Microsoft.

Further information regarding Microsoft's policies on Acceptable Use, Terms of Use, Privacy and Trademarks can be found
here: (http://www.microsoft.com/online/legal/v2/?docid=13&langid=en-us)

2.4 Data Purging

Office 365 Accounts

Email messages held under Office 365 Accounts will be subject to Microsoft's storage and retention policies, which may change from time to time, with or without notice. As of this writing, retention times are unlimited and storage limits are: Office 365 - 50GB.

2.5 Record Retention

It is the responsibility of employees to preserve College records, including emails or instant messages in particular circumstances:

- Those who have actual knowledge of matters in which it can be reasonably anticipated that a court action will be filed.
- A subpoena has been served or notice of same has been given.
- Records are sought pursuant to an audit or similar pending or possible investigation.

2.6 Data Backup

College Exchange Email Accounts are backed-up on a regular basis as a way of recovering from a systematic loss affecting the entire email system. User files and folders are not backed-up individually. Because restoration of the entire email system is a lengthy process, requests for email account restoration is generally granted only in the case that loss of the data significantly affects a business IT.

Restoration services for Office 365 Accounts are only offered for messages that have been deleted no longer than 25 days.

2.7 Expiration of Accounts

Individuals may leave the College for a variety of reasons, which gives rise to differing situations regarding the length of email privileges or expiration of accounts. The policy governing those privileges are set forth below. Notwithstanding the guidelines below, the College (IT, President

EVP, VP, Dean of Students, or other Department Heads) reserves the right to revoke email privileges at any time.

- **Faculty who leave before retirement** – Faculty who leave the College will have email privileges removed effective on their last worked day. If such separation is for cause, email privileges may be immediately revoked without notice. If the faculty members mailbox must be retained that department can request IT to transfer rights to another faculty member or have their email forwarded to another faculty member.
- **Staff who leave before retirement** – Staff members who leave the College will have email privileges removed effective on their last worked day. If such separation is for cause, email privileges may be immediately revoked without notice. If the staff members mailbox must be retained that department can request IT to transfer rights to another staff member or have their email forwarded to another staff member.
- **Retired Faculty** – Faculty who have retired from the College and granted Emeritus status will be permitted to retain their email privileges if their account remains active. All email accounts that are inactive for a period of one year will be removed.
- **Retired Staff** – Staff who have retired from the College will have email privileges removed effective on their last worked day. If the staff members mailbox must be retained that department can request IT to transfer rights to another staff member or have their email forwarded to another staff member.
- **Students who graduated** – Will be able to keep their accounts for 3 months after graduation date in order to save any data.
- **Students who leave before graduation** – Students who leave the College without completion of their degree or other program will have all email privileges terminated immediately unless requested by the Dean. The students will have a week from their separation date to remove all data.
- **Expelled students** - If a student is expelled from the College, email privileges will be terminated immediately upon the directive of the Academic Records office.

2.8 Appropriate Use and User Responsibility

No data that is classified as Protected by the Data Classification Policy shall be stored in or transmitted via email. This includes but is not limited to personally identifiable information, Social Security number, bank account information, tax forms, background checks, sensitive research data, or other Protected Data. See the College Data Classification Policy for further information.

Users who use email communications with persons in other countries should be aware that they may be subject to the laws of those other countries and the rules and policies on others systems and networks. Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts and licenses applicable to their particular uses.

Approval and transmission of email containing essential College announcements to students, faculty, and /or staff must be obtained from the Vice President for Marketing/Communications, the Vice President for Information Technology/CIO or the responsible College official noted as follows:

- For sending to all faculty, approval from the Academic Dean is required
- For sending to all staff, approval from the Vice President of that department is required
- For sending to all students, approval from the Vice President of Student Life is required

Use of distribution lists or 'reply all' features of email should be carefully considered and only used for legitimate purposes as per these guidelines.

Any use of a College Email Account to represent the interests of a non-College group must be authorized by an appropriate College official.

In order to prevent the unauthorized use of email accounts, the sharing of passwords is strictly prohibited. Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is assumed to have been authored by the account holder, and it is the responsibility of that holder to ensure compliance with these guidelines.

Email services are available for faculty and staff to conduct and communicate College business. Incidental personal use of email is allowed with the understanding that the primary use be job-related, and that occasional use does not adversely impact work responsibilities or the performance of the network.

Email services are provided only while a user is employed by the College and once a user's electronic services are terminated, employees may no longer access the contents of their mailboxes, nor should they export their mailbox to a personal account before departure.

IT maintains the College's official email systems; faculty, staff and students are expected to read email on a regular basis and manage their accounts appropriately. An email message regarding College matters sent from an administrative office, faculty, or staff member is considered to be an official notice. Faculty, staff, or students who choose to use another email system (apart from the Gmail Accounts) are responsible for receiving College-wide broadcast messages and personal mail by checking the College's official email system and the College's World Wide Web Homepage.

2.9 Departmental Accounts

Requests for shared departmental accounts will be accommodated, but require a designation of an account holder, who will administer the addition, deletion, or modification of names within the account, as well as manage the account as per these guidelines. Supported types of shared accounts are designated as:

- Type 2 – This account will be able to receive mail from anywhere on the Internet, and will be able to respond directly to the sender. The generic id will be unable to access any of the predefined mailing groups that exist within the campus environment. Members of the group/organization utilizing this type of generic id will authenticate to the Type 2 account utilizing their own personal user ID and password. Mail sent from the generic id

will not reflect the identity of the responder, but will instead carry the identity of the generic id.

2.10 Personal Email Accounts

In order to avoid confusing official College business with personal communications, employees must never use non-College email accounts (e.g. personal Verizon, Comcast, etc.) to conduct Thiel College business.

2.11 Inappropriate Use

With respect to College Email Accounts, the exchange of any inappropriate email content outlined below and described elsewhere in this policy, is prohibited. Users receiving such email should immediately contact IT, who in certain cases may also inform the Department of Public Safety, The Department of Human Resources, The Dean of Students or The Office of General Counsel.

The exchange of any email content outlined below is prohibited:

- Generates or facilitates unsolicited bulk email;
- Infringes on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;
- Violates, or encourages the violation of, the legal rights of others or federal and state laws;
- Is for any malicious, unlawful, invasive, infringing, defamatory, or fraudulent purpose;
- Intentionally distributes viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- Interferes with the use of the email services, or the equipment used to provide the email services, by customers, authorized resellers, or other authorized users;
- Alters, disables, interferes with or circumvents any aspect of the email services;
- Tests or reverse-engineers the email services in order to find limitations, vulnerabilities or evade filtering capabilities;
- Constitutes, fosters, or promotes pornography;
- Is excessively violent, incites violence, threatens violence, or contains harassing content;
- Creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement;
- Improperly exposes trade secrets or other confidential or proprietary information of another person;
- Misrepresents the identity of the sender of an email.

Other improper uses of the email system include:

- Using or attempting to use the accounts of others without their permission.
- Collecting or using email addresses, screen names information or other identifiers without the consent of the person identified (including without limitation, phishing, spidering, and harvesting);

- Use of the service to distribute software that covertly gathers or transmits information about an individual;
- Conducting business for profit under the aegis of the College
- Political activities, specifically supporting the nomination of any person for political office or attempting to influence the vote in any election or referendum on behalf of or under the sponsorship of the College.

This list is not intended to be exhaustive but rather to provide some illustrative examples.

3. Scope

This policy applies to all individuals who use or maintain a Thiel College provisioned email account.

4. Procedures

IT staff can provide recommendations and support for this policy through specific considerations and technologies.

4.1 SPAM & Phishing

All incoming email is scanned for viruses, phishing attacks and SPAM. Suspected messages are blocked from the user's inbox. Due to the complex nature of email, it is impossible to guarantee protection against all SPAM and virus infected messages. It is therefore incumbent on each individual to use proper care and consideration to prevent the spread of viruses. In many cases, viruses or phishing appear to be sent from a friend, coworker, or other legitimate source. Do not click links or open attachments unless the user is sure of the nature of the message. If any doubt exists, the user should contact the Solution Center at support@thiel.edu.

SPAM messages can be forwarded to support@thiel.edu where they may be added to the filter list.

5. Definitions

SPAM is defined as unsolicited and undesired advertisements for products or services sent to a large distribution of users.

Phishing is defined as the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.