We write to inform you of a new **password policy** that takes effect **March 1, 2021**.

Information Technology had a Penetration Test done by TCM Security to test our security controls in place to protect and secure the institution's information assets. An observation of this Penetration Test has identified that Thiel College's password length and complexity does not meet current security requirements; a best practice that is one of many measures to safeguard our information. You can read more about Penetration Testing at https://tcm-sec.com/service-post/external-penetration-testing/.

To address this concern, we are implementing a new password policy whereby **all faculty and staff** will be required to **change their password from 8 characters in length to 12**. This requirement seems to be consistent with other higher education institutions that have password policies in place. A password change will still be required every 90 days. Also, a **Password Filter** will be put in place to ban common and easily guessed passwords such as Thiel, Tomcats, Building Names, Seasons, Months, Years, Sport Terms/Teams, and Fantasy Characters.

Multi-Factor Authentication will also be enabled when this change occurs. More information can be found at https://www.thiel.edu/mfa. A separate email will come out explaining that in more detail.

Students will have to adhere to the same policy with the exception that their passwords will not expire.

Systems that will be affected by this password change include email (Office 365), Active Directory (access to your computer), The Hub, Moodle, Thiel Wireless, and VPN.

It should also be noted a password history will be kept, whereby you cannot simply alternate between two passwords. The history will be set to five passwords, which in reality means that after the sixth password change, you could resume using your first password.

The new policy will go into effect on **March 1, 2021**. Notification email will be sent to faculty and staff whose password is approaching the expiration time. Being sensitive to the phishing types of messages that ask for credentials (user name and password), the message will be just like the normal password reset email, simply stating that your password is about to expire.

We realize that this new policy will cause some inconvenience, but it is one of the safeguards that is a best practice towards securing our information assets. If you have any questions about the policy you may direct them to the Solution Center at support@thiel.edu or x4000.

More information can be found at https://www.thiel.edu/offices/information-technology/policies-and-procedures.

Thank you for your help in our ongoing information security efforts at Thiel College. We are sincerely trying to balance security, privacy, and our culture of open access.