1. Seton Hall Information Technology - User Responsibilities Form V1.3

All users of the University's computer systems must handle essential University information in a professional and secure manner. Individuals may access only information and systems they have authorization for, and may use information only for appropriate business or academic purposes. Specific responsibilities include:

1. Users are forbidden from disclosing sensitive information to anyone who does not have a business or academic need to know, including:
    a. Personally identifiable information (names, Social Security numbers, addresses, telephone numbers, driver's license numbers, credit card information, etc.) that they may have access to in the normal course of doing business; and
    b. Confidential University information (enrollment projections, budget projections, grades, payroll information, etc.) that they may have access to in the normal course of doing business.
    c. Information protected by state and federal regulation, such as students' academic and financial records.
2. Network and application passwords must:
    a. Never be shared with anyone
    b. Not be composed so that they can be easily guessed; they should be a minimum of eight characters long, with at least one uppercase and one lowercase alphabetic character plus at least one numeric character, with not more than two consecutive repeating characters; and
    c. Be changed at least every 180 days to a password not previously associated with that account.
3. Users must not make, accept, or use unauthorized copies of software or download any unauthorized programs from the Internet and ensure that license agreements are not purposefully violated.
4. All downloads and media should be scanned for viruses prior to use, and all virus and security incidents must be reported immediately after occurrence.
5. Confidential information should not be sent unprotected over the Internet, stored unencrypted on an unsecured computer or an unsecured external storage medium or device, or communicated using a unauthorized third party email or social networking system.
6. Vital information on standalone PCs or workstation hard drives should be backed up when it is created and whenever it is significantly changed; copies should be moved as soon as possible to a physically secure location, such as a network drive or a hard drive in a secured location.
7. Security incidents or suspected violations of the security policy should be reported to the University's Information Security Officer or other appropriate manager.

As User of SHU Technology assets, I acknowledge the above and will comply with the best of my ability.

Name: _____ *(please print)*

*Sign:*_____ *Date:*_____