



## User Accounts and Password Policy

Last Modified: October 12, 2020

Hofstra University values the security of confidential information maintained on its computer systems. In order to maintain system security, access to Hofstra University's computer systems is restricted to those users who have an account and password. Hofstra University provides user accounts and passwords to employees in order to perform University-related business operations. While incidental use of University computer systems is permitted, the management and usage of these accounts is governed by University policies.

A user account is a privilege granted to a specific user, and the sharing of that account is a violation of University policy. All users are responsible for taking the appropriate steps to protect their user accounts and passwords. Users will be held responsible for the activities that are performed by their account.

User accounts remain active for only as long as the user is authorized to access University resources. Once a user leaves the University or is reassigned to responsibilities in which the account is no longer required, the account is deactivated. Users are only provided access (i.e., privileges) to computer resources that are required to perform their job responsibilities.

### **The following are guidelines to protect user passwords:**

1. Users should exercise caution in keeping their passwords confidential. Passwords should not be written down or shared with anyone, including technical staff.
2. Users who suspect someone may have knowledge of their password should change it immediately through the Hofstra Portal (<https://www.hofstra.edu/password>), which contains self service instructions for changing a password. Users who continue to have problems should contact the University's Help Desk (Ext: 3-7777).
3. Users should choose strong passwords. Example: Do not use common or simple words, such as "secret" or "private" as your password. In addition, avoid passwords that contain personal information, such as your name, birthday, address, Social Security Numbers, etc.
4. To assist users in selecting strong passwords, the University requires passwords to have a minimum of at least eight (8) characters; the first character cannot be numeric, and the password must contain at least one number and a special character (e.g., "!", "\*", etc).
5. Users should not use the "Remember Password" feature in web browsers, e-mail software, or other programs that connect to the Internet. Often these features store passwords in an unprotected manner, which may allow others that use the computer to view it.

6. Hofstra usernames and passwords should not be used for personal accounts. Users should create a different username and password for external services such as personal e-mail accounts, online stores, banking, music services, Web sites, personally owned computers, or other systems. This will prevent others who are outside the University from associating a user to their Hofstra user account (e.g., an outsider attempting to access University systems by using a Hofstra user ID and password on the Public Hofstra Web Portal).