Hofstra University
Confidentiality Agreement and Security Policy

Hofstra University regards security and confidentiality of data and information to be of utmost importance. As such, the University requires all users of data and information to follow the procedures outlined below:

Policy on Confidentiality of Data

Each employee, consultant, student, or person granted access to data and information holds a position of trust and must preserve the security and confidentiality of the information he/she uses. Users of University data and information are required to abide by all applicable Federal and State guidelines and University policies regarding confidentiality of data, including, but not limited to the Family Education Rights and Privacy Act (FERPA). All users of University data and information must read and understand how the FERPA policy, located at www.hofstra.edu/policies, applies to their respective job functions.

Any employee or person with authorized access to Hofstra University's computer resources, information system, records or files is given access to use the University's data or files solely for the business of the University. Specifically, individuals should:

a. Access data solely in order to perform his/her job responsibilities.
b. Not seek personal benefit or permit others to benefit personally from any data that has come to them through their work assignments.
c. Not make or permit unauthorized use of any information in the University's information system or records.
d. Not enter, change, delete or add data to any information system or files outside of the scope of their job responsibilities.
e. Not include or cause to be included in any record or report, a false, inaccurate or misleading entry.
f. Not alter or delete or cause to be altered or deleted from any record, report or information system, a true and correct entry.
g. Not release University data other than what is required in completion of job responsibilities.
h. Not exhibit or divulge the contents of any record, file or information system to any person except as it is related to the completion of their job responsibilities.

Additionally, individuals are not permitted to operate or request others to operate any University data equipment for personal business, to make unauthorized copies of University software or related documentation, or use such equipment for any reason not specifically required by the individual's job description.

It is the employee's responsibility to report immediately to his/her supervisor any violation of this policy or any other action, which violates confidentiality of data.

Security Measures and Procedures

All users of University information systems are supplied with a network account to access the data necessary for the completion of their job responsibilities. Users of the University information systems are required to follow the procedures outlined below:

1. All transactions, processed by a user ID and password, are the responsibility of the person to whom the user ID was assigned. The user's ID and password must remain confidential and must not be shared with anyone.

   - Do not use anyone else's password. Using someone else's password is a violation of policy, no matter how it was obtained.
   - Do not share your password with anyone. Your password provides access to information that has been granted specifically to you. To reduce the risk of shared passwords – remember not to post your password on or near your workstation.
   - It is your responsibility to change your password immediately if you believe someone else has obtained it.

2. Access to any student or employee information (in any format) is to be determined based on specific job requirements. The appropriate Director, Dean, Provost, and/or Vice President are responsible for ensuring that access is granted only to authorized individuals, based on the performance of their job. Written authorization must be received by the Computer Center prior to granting system access.

   You are prohibited from viewing or accessing additional information (in any format) unless you have been given the proper written authorization. Any access obtained without written authorization is considered unauthorized access.

3. In order to prevent unauthorized use, the user shall log off of all applications that are sensitive in nature, such as Hofstra Online Information Systems (Banner), when leaving the workstation. Locking screen savers are automatically invoked after 15 minutes of activity. (Faculty workstations are set to a 15 minute timeout but they have an option to request through the Helpdesk to extend the timeout to 30 minutes.)

4. Passwords are set to be changed by the system every 6 months and immediately if there is reason to believe they have been compromised or revealed inadvertently. If you need help in changing your password, please call the Help Desk at x3-7777. Additionally, notify your supervisor immediately if you suspect unauthorized use of your password.

5. Upon termination of an employee, Human Resources emails a Clearance notification to all of the Information Technology groups required to perform clearance activities including but not necessarily limited to retrieval of University assets, account deletion or suspension, removal of application/storage/access rights, updating information services, et al.

   Upon transfer of an employee, Human Resources emails a Campus Relocation notification to all of the Information Technology groups required to perform transfer/relocation activities including but not necessarily limited to modification and/or removal of rights, updating information services, et al.

6. Generally, students and temporary employees should not have access to the University record system. **Written approval of the Vice President or Dean and Provost in charge of the respective department is required** if it is determined that access is required. The student or temporary employee is to be held to the same standards as all University employees, and must be made aware of their responsibilities to protect student and employee privacy rights and data integrity. Written authorization must be received by the Computer Center prior to granting system access.

Additionally, I understand that if granted access to process transactions via Banner Web, I have access to a secure information area. Any information I enter or change will be effective immediately. Accordingly, I understand that I am responsible for any changes made using my ID. I agree not to share my ID or PIN number with any other individuals and will notify Human Resources immediately if I believe my password has been compromised.

Hofstra University
Confidentiality Agreement and Security Policy

I understand that my access to University data and information systems is for the sole purpose of carrying out my job responsibilities. Breach of confidentiality, including aiding, abetting, or acting in conspiracy with any other person to violate any part of this policy, may result in sanctions, civil or criminal prosecution and penalties, employment and/or University disciplinary action, and could lead to dismissal, suspension or revocation of all access privileges. I understand that misuse of University data and information and any violation of this policy or the FERPA policy are grounds for disciplinary action, up to and including, dismissal.

I have read the above and agree to comply with Hofstra University's Confidentiality Agreement and Security policy, and any updates or revisions published or posted to www.hofstra.edu/policies.

……..
Employee Name (Please Print)

……..
Employee Signature

……..
Department

……..
Date