Instructions

1. Print the form, read the data security policies on the UISO “Policies” web page at: http://security.georgetown.edu/page/1242736355584.html and the Confidentiality Agreement on the reverse, sign the form, and then have your supervisor or department chair/program director countersign the form. If you are part of the Biomedical Group, you also need to have the Director for Biomedical Graduate Education (BGE) sign the form.

2. After the form is completed and signed, you should scan and send it as a PDF to gradmail@georgetown.edu (Subject: AY Setup). You may also FAX the form(s) to the Graduate School (fax: 202-687-6802); or MAIL/DROPOFF at the Graduate School in Car Barn, Suite 207 (Attn: AY Setup) for processing.

3. Graduate School staff will review and submit the form for final approval by the Admissions Data Steward (Jennifer Hunt). Once approved by the Admissions Data Steward, the ApplyYourself account will be setup and you will be contacted.

By signing and submitting this form, I agree to abide by all University policies, procedures, terms and conditions pertaining to confidentiality and protection of data listed on the University Information Security Office “Policies” webpage at http://security.georgetown.edu/page/1242736355584.html including the information summarized in the Confidentiality Agreement printed on the next page. In the event that my duties no longer include graduate admissions for this department/program, or I terminate my employment with Georgetown University, I will immediately notify the Graduate School so that they may modify/inactivate my account. I also agree to attend a University Information Security Office training session on Data Security Guidelines and Policies.
CONFIDENTIALITY AGREEMENT:
All employees of Georgetown University (academic, administrative, staff and student workers) are required to abide by the policies and procedures governing review, release, retention and protection of student education records. The federal regulations governing use of this data include, but are not limited to, the following:

- **Family Educational Rights and Privacy Act of 1974 (FERPA)**, which mandates that information contained in a student’s education record must be kept confidential and outlines the procedures for review, release and access of such information;
- **Gramm-Leach-Bliley Act of 1999 (GLBA)**, which requires that the University protect what non-public personal information (NPI) they share about customers with third parties and that the University provide security and integrity of customers’ NPI and data.
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**, which governs the ways in which the University can use, keep, and disclose health information.

Access to the Banner Student System will be granted to those individuals who have been determined to have a legitimate educational interest (as defined in FERPA) and business need for the data. Access to specific student data will only be granted with the approval of your supervisor and the appropriate Data Steward(s) as custodian(s) of this data.

Individuals who have been granted access to any part of the Banner student system (or other systems containing non-public personal information such as admissions applications and data) must understand and accept the responsibility of working with confidential student records. Users applying for Banner accounts agree to attend a University Information Security Office training session on Data Security Guidelines and Policies. The following rules apply:

- Your access to the system is based on your NetID.
- If you are a Banner user, you will need a separate password. This password must not be your NetID password. As with all passwords, this password must be kept confidential and may not be shared or given to anyone, including supervisors, co-workers, student employees, or friends.
- You must use only your own account. When access to additional screens or systems is needed, you must request it through your supervisor to the appropriate Data Steward(s).
- You are responsible for any data that is accessed, changed or retrieved using your account.
- You are required to keep your password confidential. If you ever suspect that your account or password is compromised, you must change your password immediately and notify the University Information Security Office.
- You may only access those records for which you have authorization that are in the scope of your assigned responsibilities.
- You may not view, print, copy, update, or disclose data for non-work-related reasons, including curiosity, even if your permissions allow such access.
- You may not, under any circumstances, view, update, or maintain your own record in Banner (or other information systems), even if your job responsibilities otherwise permit access to your record (this excludes allowed access to your personal employee GMS account and to your Banner MyAccess account).
- You are responsible for adhering to all policies and regulations governing confidential data, including (but not limited to): Acceptable Use Policy, Information Security Policy, Interim Policy on the Use, Collection, and Retention of Social Security Numbers, Incident Reporting Procedures, Record Retention Policy, Procedures for the Protection of University Information, and others. Complete links to these and other policies are located at: [http://security.georgetown.edu/page/1242736355584.html](http://security.georgetown.edu/page/1242736355584.html)

A complete policy statement on the Georgetown University implementation of FERPA guidelines can be found in the appropriate School bulletin or handbook. In part, the policy states that officials of the University will be given access to student education records on a “need-to-know” basis and that such access must be limited to those with a legitimate educational interest (as defined in FERPA) in the student whose information is accessed. The information contained in a student’s education record may not be released to a third party without the written consent of the student. The only exception is directory information defined as the student’s name, local and home addresses and telephone numbers, major field of study, dates of attendance, degrees and awards received.

Individuals using these systems are subject to having all of their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring. Misuse of the system, may result in loss of access and/or be subject to disciplinary action by the University. Be advised that if monitoring reveals possible evidence of criminal activity, the University may be required, upon request, to provide records to law enforcement officials.