



# Banner Account Application

## Division of Information Technology

Carter Hall • (910) 775-4340 • [doit@uncp.edu](mailto:doit@uncp.edu) • <http://www.uncp.edu/doit>

**Submit the original hard copy to the DoIT main office (Carter Hall)**

Use this form to apply for a Banner account (not a Self Service Account). Use a separate application for each instance. This application should be accompanied by at least one Banner Class Assignment Application. Approval of this application provides the applicant with a Banner account, but does not afford access to any Banner objects or data. Banner Class Assignment Applications must be approved by the appropriate Data Manager. A current list of Data Managers is available at <http://www.uncp.edu/doit/banner/managers.html>.

### APPLICANT

<i>Last Name:</i>	<i>First Name:</i>	<i>Middle Name:</i>
<i>Department:</i>	<i>Campus Phone:</i>	<i>Banner Instance:</i>

### CONDITIONS OF THIS APPLICATION

This is an application to access information systems of the University of North Carolina at Pembroke. Access to these systems is governed by federal legislation, including but not limited to, the Family Education Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Gramm-Leach-Bliley Act of 1999 (GLBA). Access is also governed by General Statutes and policies of the State of North Carolina as well as policies and procedures of the University of North Carolina, UNC Pembroke and the Office of the Division of Information technology.

### RESPONSIBILITIES OF USERS

Users assume the responsibility for their actions and are required to follow sound, secure and ethical computing practices as outlined in the UNCP Appropriate Use Policy (DOIT 0103), available at <http://www.uncp.edu/doit/policies/policy0103.html>. Users may not access any data or systems unless they have been granted explicit permission for such access. Users must protect the privacy and security of data and must guard against its theft, loss or accidental disclosure. Users must safeguard all data, whether stored on servers, local machines, on portable media, or in print. Users must not share passwords or provide access to others. Users must not distribute or disclose data to other parties without approval of the appropriate the Data Manager. Users must not attempt to alter, circumvent, disable or remove system or network security safeguards. Users must promptly report any violations of policy or procedures to the Division of Information technology. Other responsibilities apply under the previously mentioned legislation, policies and procedures.

By signing this document, the applicant agrees to abide by these conditions and acknowledges that he or she has not altered this document from its original form.

\_\_\_\_\_  
*Signature of Applicant*

\_\_\_\_/\_\_\_\_/\_\_\_\_  
*Date*

\_\_\_\_\_  
*Signature of Supervisor*

\_\_\_\_/\_\_\_\_/\_\_\_\_  
*Date*

### Division of Information technology Use Only

\_\_\_\_\_  
*Banner Access Control Approval*

\_\_\_\_\_  
*Date*

\_\_\_\_\_  
*Username*

\_\_\_\_\_  
*Completed*

\_\_\_\_\_  
*Date*

\_\_\_\_\_  
*Account Type*