Hampton University
Request for Internal Training of Employee (v6)

An online form

Attendee/Employee Information

Name (First, Middle, Last)   **EmpID#**   **Dept#**   **Phone**

Title   **Department**

Employee Function/Job Duties   **Requested Training Date**

Previous Sign-in Names in Banner

Employee Status		Banner Security	
New employee:			
Position Change	Transfer /Hire Date		Copy Banner profile
Employee replaces →			
Current Employee			

Finance Security
Budget/Account Number
(Finance Must Approve Access)

Temporary Employee HUID # _____

TEMP HR Approved **(HR must approve Banner access prior to any access/training)**

_____
HR Printed Name and Signature of Approval Authority

_____
Finance Printed Name and Signature of Approval Authority

Training	Initial Banner Modules
☐ Navigation	☐ Student
☐ Budget	☐ Financials
☐ On-Line Requisition	☐ Alumni
Argos Reporting	☐ Human Resources
	☐ Financial Aid

Index	Fund	Organization	Type of Access Query/Modify/Both

☐ **Check if additional account numbers are attached to this form**.

System accounts will not be generated for persons not employed by Hampton University. Only staff persons who can be successfully verified as Hampton University employees through the Human Resources System, or through documentation such as contracts will receive access to M.I.S resources. User IDs generated for temporary employees or staffing persons will be at the risk of the department's supervisors and the agency at which the person is employed. Therefore the agency is liable for damages to information and or resources.

Supervisor's Printed Name and Legal or Electronic Signature (Required)   **Phone #**   **Date**

This certifies that I _____ will complete training as requested above by my supervisor.
Print Name First, Middle, Last (Required)

I have read and understand that access to computer systems and networks owned or operated by Hampton University imposes certain responsibilities and obligations and are subjected to other university policies, local, state, and federal laws. I understand acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. I am also held accountable for the use of any ID that I will use or have been assigned. It is my responsibility to protect the integrity of accessible systems and to preserve the confidentiality of accessible information as appropriated. I understand my duties and responsibilities in enforcing the Hampton University's Policy on Confidentiality and Security of the University's Information Systems. In addition my signature certifies that I have completed training as requested by my above supervisor. I also understand training is a pre-requisite and is a requirement for my position and is subject to change as required by my position.

Employee Legal or Electronic Signature (Required)   Date

ERP Banner Team use only
Banner 9 Training Class Completed   **Date completed**

☐ Banner Navigation and General Person
☐ Hampton University Data Standards
☐ Banner Financials – Budget /Grant Management (optional)

Trainer's Printed Name and Signature
Date Completed   Completed By

Reference: Request for Training Policy

Hampton University's			
Policies & Procedures for Information Technology			
Date		**Department**	Computer Center
Policy	Confidentiality and Security of Information Systems	**Policy No:**	001.00A

I _____

Print Name (First, Middle, Last) Required

have read and understand the above policy and procedure. I also understand that access to computer systems and networks owned or operated by Hampton University imposes certain responsibilities and obligations and are subjected to other university policies, local, state, and federal laws. I understand acceptable use always is ethical, reflects academic honesty, and shows restrain in the consumption of shared resources. I am also held accountable for the use of any ID that I will use or have been assigned. It is my responsibility to protect the integrity of accessible systems and to preserve the confidentiality of accessible information as appropriate. I understand my duties and responsibilities in enforcing the Hampton University's Policy on Confidentiality and Security of the University's Information Systems.

_____

Legal or Electronic Signature **(Required)**　　　　HUID #　　　　Date

Violation
Violations or suspected violations of the policies enumerated above should be reported promptly to the Director of Management Information Systems @ 728-6544 or the Assistant Provost for Information Technology @ 728-6988

v

BDS 001.00 ver. A Path: \groups\policies

Hampton University's			
Policies & Procedures for Information Technology			
Date		**Department**	Computer Center
Policy	Confidentiality and Security of Information Systems	**Policy No:**	001.00A

Statement of Policy

It is the policy of Hampton University to control computer system access to sensitive information in order to maintain confidentiality, and data integrity. Sensitive information can relate either to student, faculty, staff, or organizational information.

Purpose

To establish guidelines for the access of sensitive information to Hampton University's Information Systems. (i.e. SIS, HRS, FRS, ADS, On Course and Intranet) and all other computer data housed on Hampton University's computers.

Procedure

I.   Security Awareness

   A.   Department heads and Faculty Chairpersons are responsible for in-servicing their employees so that the employees understand the security policies and procedures to be followed.

   B.   Employees assume the responsibility for the security of all operations (processes) and assets (data) entrusted to their care.

   C.   Employees must keep user ID's, logons, passwords, and methods used to access Information Systems resources and facilities confidential.

   D.   Employees are required to exercise due diligence to prevent unauthorized disclosure or improper manipulation of information for any purpose not specifically intended by the University.

   E.   Employees must notify a responsible person (e.g., Information Systems or a department head) of suspected system abuse.

   F.   Department Heads must notify Information Systems when an employee terminates or transfer from the department.

II.   Information Security Exposures, which may result in disciplinary action, including immediate termination.

   A.   **Information disclosure.**   Unauthorized disclosure can affect any organization's profitability. If confidential information is released without the consent of the

Violation
Violations or suspected violations of the policies enumerated above should be reported promptly to the Director of Management Information Systems @ 728-6544 or the Assistant Provost for Information Technology @ 728-6988

BDS 001.00 ver. A Path: \groups\policies

party, used for personal gain or for malicious purposes, then this type of behavior can affect the University legally.

B. **Corruption of data or programs.** Modification or altered documents, computer programs, data files, transactions, or reports can result in misstated assets, erroneous student information, erroneous management of planning and control data, or be used to conceal possible fraud.

C. **Destruction of physical assets or information.** Business can be seriously interrupted or indefinitely curtailed depending on the degree of information or processing dependency, the target, and extent of destruction.

D. **Interruption of service.**   Interruption of processing schedules can impair or curtail basic service and product delivery.

E. **Removal of physical assets or information.** Unauthorized removal of hardware components or storage media can seriously disrupt an organization's ability to continue normal business operations.

F. **Unauthorized use of passwords.**   Unauthorized use or disclosure of passwords can result in disclosure or improper manipulation of information.

III. Access

A. Employees will be given access to the computer systems necessary to perform their position functions.

B. For stand alone systems without password security these simple precautions:
1. Take sensitive data off the hard disk and lock it away.
2. Avoid readily understandable labels on diskettes containing sensitive data.
3. Take good care of diskettes, file away properly, and index and label them clearly.
4. Use write-protect tabs to prevent accidental erasure. Also, use other software locks designed for the same purpose such as a document password in MS WORD and the protect feature in EXCEL.
5. Use code words for confidential files, both in the computer and file cabinets. (Set this up with your supervisor.)
6. Take a periodic inventory of hardware and software.
7. Lock rooms containing valuable equipment.
8. Do a periodic self-audit of your security procedures.

C. For all systems with password security:
1. The systems and information to which an employee has access to will be determined by their position function.

Violation
Violations or suspected violations of the policies enumerated above should be reported promptly to the Director of Management Information Systems @ 728-6544 or the Assistant Provost for Information Technology @ 728-6988

BDS 001.00 ver. A Path: \groups\policies

        2.   Recommended security levels by position are available from Information Systems. Do not exceed the recommended levels without attaching justification.

        3.   Department Heads will complete and send to Information System the Information Systems Access Form for each employee.

        4.   Non-employees may be issued temporary password. Please attach justification with a form and to date for access.

        5.   Information Systems will review the request and, if determined appropriate, complete the request, and/or route it on to the Systems Administrator and or person(s) responsible for updating password files. (i.e. Information Technology Center, Computer Information Center).

        6.   Information Systems will file the original request and notify the Department Head.

        7.   The Department Head is responsible for informing the employee of the password.

IV.   Password/Access Information

     A.   Employees must contact Information Systems in person if they forget their logon or passwords.

     B.   Departments should keep a list of user logons and the master password in a secure file.

V.   Other Security Measures

     A.   Information Systems passwords will be automatically set to require a password change every 3 months.

     B.   An employee's password will be deleted at the request of a department head, when Information Systems determines that the password has been used inappropriately, and upon termination.

     C.   Information Systems will review the payroll termination report at least quarterly in order to delete passwords and user Ids.

     D.   When available, the intruder lockout will be set to three tries before shutting down the workstation.

     E.   Concurrent logons will be set to 1 so that user may only log onto one terminal at a time.

VI.   Access to Computer System Reports

     A.   On-line reports are controlled by password security and or user access level.

Violation
Violations or suspected violations of the policies enumerated above should be reported promptly to the Director of Management Information Systems @ 728-6544 or the Assistant Provost for Information Technology @ 728-6988

BDS 001.00 ver. A Path: \groups\policies

B. Batch and "greenbar" reports are distributed by Information Systems. Information Systems uses common sense for approving distribution of reports. If Information Systems determines that the report is not necessary for your position function you will need to submit a letter from a vice president in order to receive the report.

C. Departments and employees are responsible for the destruction of reports with sensitive and confidential information.

Violation
Violations or suspected violations of the policies enumerated above should be reported promptly to the Director of Management Information Systems @ 728-6544 or the Assistant Provost for Information Technology @ 728-6988

BDS 001.00 ver. A Path: \groups\policies