|  |
| --- |
|  *Communications and Information Technologies(CIT)* Banner : Operating System Shell Management Policy  |
| Purpose | The purpose of this policy is to establish standard practice for operating system account management for shell access to the Banner system environment. |
|  |
| Scope | This policy applies to all Faculty, Staff, Students, and/or Vendors of the University that use the Banner system via operating system shell account access. Operating systems levels access is currently only available via secure shell encrypted access mode. |
|  |
| Policy | Requests are made via email to include a completed Banner Operating System Account Request / Change Form and Employee Confidentiality Agreement. Both of these forms are generally available on-line at <http://www.tnstate.edu/cit/banneraccess.aspx>. |
|  |
| Procedures | * The Employee will complete the Employee section of the Banner Security Request /Change Form.
* The Supervisor will complete the Supervisor section of the Banner Security Request Form.
* The Supervisor will then forward the Banner Security Request Form to the Banner Area Security Officer by email. This email will also state the business need of the Employee.
* The Banner Area Security Officer will complete the Banner Area Security Officer section of the Banner Security Request Form.
* The Banner Area Security Officer will then email the Banner Security Request Form to CIT Systems Manager and carbon copy MIS Management. The Banner Area Security Officer will retain a copy of the Banner Security Request Form.
* After ensuring that the Banner Security Request Form and Employee Confidentiality Agreements have both been received, CIT Systems to perform the requested security action.
* CIT Systems will complete the Systems section of the Banner Security Request Form. CIT Systems and MIS will retain a copy of these forms.
* CIT Systems will send an email to the Banner Security Officer and the Employee informing them of the completion of the request.
* In the case of the creation of a new Banner account or password reset, CIT Systems will send an email to the Employee with login instructions.
* In the case of an Employee separation from TSU, CIT Systems will receive an email from esa@tnstate.edu with information regarding the Employee. MIS will complete the Employee and MIS portions of the Banner Security Request Form. CIT Systems will lock the system shell account and will retain a copy of this form and the email from ESA.
 |

Revised 02/26/2013

|  |
| --- |
|  *Communications and Information Technologies(CIT)* Banner : Operating System Shell Management Policy  |
| Terms and Conditions | * Only CIT staff will have access to banner system accounts named “oracle” and “banner”.
* CIT staff must execute “su” in order to use the oracle and banner account roles
* CIT MIS department will be responsible for sharing the “oracle” and “banner” account passwords with CIT MIS employees.
* All shell accounts will include standard shell logging.
* A notice of university computing no expectation of privacy notice may be included on the system login page.
* A notice of university acceptable use may be included on the OS system login page.
* All users should exerciser appropriate caution to avoid any data corruption or loss, since system backups are only intended for disaster recovery mitigation.
* All data on the system are subject to the university confidentiality agreements as well as relevant state and federal rules and regulations.
 |

Revised 02/26/2013