From: UGA Business Services info. <BUSINESS-SERV-L@LISTSERV.UGA.EDU> on behalf of Holley W Schramski <hschrams@UGA.EDU>
Sent: Tuesday, May 14, 2013 5:24 PM
To: BUSINESS-SERV-L@LISTSERV.UGA.EDU
Subject: New USG User Account Standards Effective July 1, 2013
Attachments: Memo-New USG User Account Standards 5.16.13.pdf

Please see the attached memo from Tim Chester, Vice President for Information Technology. The text of the memo is included below for your information.

The University System of Georgia (USG) has released new standards regarding user account management for information systems containing restricted or sensitive data. Effective July 1, 2013, the University of Georgia is required to implement these standards by adhering to the following administrative procedures.

- Employees who leave the University must have their access to systems containing restricted and sensitive information removed no more than five (5) business days after the effective date.

- Employees who change departments within the University must have their access to systems containing restricted and sensitive information updated to reflect their new duties within thirty (30) days of the effective date. Employees who change jobs within the same department should have their account permissions reviewed within the same 30-day period.

- Units maintaining information systems containing restricted and sensitive information are required to review all user access every four months, making adjustments as appropriate, and document their findings with their campus information security officer. At UGA, the associate CIO for university information security will maintain this information.

To provide support to units in meeting these requirements, EITS has implemented new procedures automating the sharing of information regarding employee departures and departmental transfers.

- Individuals responsible for information systems containing sensitive or restricted information will be required to join a listserv where they will be provided daily reports on employees who have left the university or who have transferred to a new Unit. EITS will be offering training for those receiving this information that will be scheduled in July. Files will be available electronically allowing Units to automate these procedures should this be desired.

- To automate these processes at the University level, EITS will take steps to deactivate mainframe user accounts (RACF) and the UGA MyID of those individuals who depart the University. The UGA MyID inactivation does not apply to students or retirees. Users who change departments will automatically have their RACF ID revoked and will be required to request new mainframe access based on their new duties.

University departments are expected to document compliance with these standards which shall be subject to inspection by University or USG auditors. For information on the complete USG standards browse to http://ow.ly/kQnvX on the Web.

Department and other Unit heads should work to identify the individuals within their areas who are the functional system owners for information systems containing sensitive and restricted information. Names of these individuals should be submitted to adminfo@uga.edu by July 1, 2013.

For more information, contact EITS Access Services at adminfo@uga.edu or 706-542-4000. You may also point your browser to the Access Services website which contains information about the USG standard, UGA procedures, and documentation on EITS supporting resources: http://eits.uga.edu/access_and_security/access_services

The University of Georgia

Office of the Vice President for Information Technology

Dr. Timothy M. Chester
Vice President for Information Technology

171 Boyd Graduate Studies
200 DW Brooks Drive
Athens, Georgia 30602
Telephone 706-542-3145
Fax 706-542-6105
tchester@uga.edu
www.eits.uga.edu/vpit

May 14, 2013

MEMORANDUM

TO: Vice Presidents, Deans, Department Heads, and Administrative Directors

FROM: Timothy M. Chester, Vice President for Information Technology

RE: New USG User Account Standards Effective July 1, 2013

The University System of Georgia (USG) has released new standards regarding user account management for information systems containing restricted or sensitive data. Effective July 1, 2013, the University of Georgia is required to implement these standards by adhering to the following administrative procedures.

- Employees who leave the University must have their access to systems containing restricted and sensitive information removed no more than five (5) business days after the effective date.

- Employees who change departments within the University must have their access to systems containing restricted and sensitive information updated to reflect their new duties within thirty (30) days of the effective date. Employees who change jobs within the same department should have their account permissions reviewed within the same 30-day period.

- Units maintaining information systems containing restricted and sensitive information are required to review all user access every four months, making adjustments as appropriate, and document their findings with their campus information security officer. At UGA, the associate CIO for university information security will maintain this information.

To provide support to units in meeting these requirements, EITS has implemented new procedures automating the sharing of information regarding employee departures and departmental transfers.

- Individuals responsible for information systems containing sensitive or restricted information will be required to join a listserv where they will be provided daily reports on employees who have left the university or who have transferred to a new Unit. EITS will be offering training for those receiving this information that will be scheduled in July. Files will be available electronically allowing Units to automate these procedures should this be desired.

- To automate these processes at the University level, EITS will take steps to deactivate mainframe user accounts (RACF) and the UGA MyID of those individuals who depart the University. The UGA MyID inactivation does not

apply to students or retirees. Users who change departments will automatically have their RACF ID revoked and will be required to request new mainframe access based on their new duties.

University departments are expected to document compliance with these standards which shall be subject to inspection by University or USG auditors. For information on the complete USG standards browse to http://ow.ly/kQnvX on the Web.

Department and other Unit heads should work to identify the individuals within their areas who are the functional system owners for information systems containing sensitive and restricted information. Names of these individuals should be submitted to adminfo@uga.edu by July 1, 2013.

For more information, contact EITS Access Services at adminfo@uga.edu or 706-542-4000. You may also point your browser to the Access Services website which contains information about the USG standard, UGA procedures, and documentation on EITS supporting resources: http://eits.uga.edu/access_and_security/access_services

CC: Business Affairs Advisory Forum (BAAF)
Identity Management Functional Advisory Committee (IDMFAC)
Information Management System Users (IMS-L)
Information Technology Managers Forum (ITMF)
UGA Networking Group (UGA Net)
Enterprise Information Technology Services (EITS-L)