

From: UGA Business Services info. <BUSINESS-SERV-L@LISTSERV.UGA.EDU> on behalf of Chad Cleveland <cleveland@UGA.EDU>
Sent: Monday, February 17, 2014 10:13 AM
To: BUSINESS-SERV-L@LISTSERV.UGA.EDU
Subject: USG User Account Standards
Attachments: Memo-USG user accounts 2.14.14.pdf

This memo is being sent on behalf of EITS and has been distributed on several listservs.

TO: Vice Presidents, Deans, Department Heads, and Administrative Directors
FROM: Timothy M. Chester, Vice President for Information Technology
RE: USG User Account Standards, Follow-Up on Requirements

Last year, the University System of Georgia released new standards regarding user account management for information systems containing sensitive or restricted information, or other systems deemed as mission-critical to the University's ability to conduct business. These standards, which were effective July 1, 2013, were implemented at UGA through an automated process that disabled user's MyID or RACF ID when they left University employment. Through this implementation, units were also provided electronic notification of employees who depart the University, allowing them to meet these requirements. For background, information on these requirements is available at <http://ow.ly/kQnvX> on the Web.

In addition to requiring that institutions disable accounts for those departing employees within five (5) business days and adjusting user permissions appropriately for employees changing University roles within thirty (30) days, these standards also require a manual review of user access for these systems every four (4) months. A manual review of user access typically requires system support personnel to audit all user accounts for a system and verify with user departments that system access continues to be required for that employee to perform their duties. EITS Access Services has typically performed this audit of mainframe accounts every twelve (12) months.

Because UGA has taken steps to automate disabling of user accounts for departing employees, USG has provided UGA with an exception to the four-month user audit and will allow UGA to complete a user access audit each year for information systems containing sensitive or restricted information, or other systems deemed as mission-critical to the University's ability to conduct business.

User departments are expected to document compliance with these standards, which shall be subject to inspection by University or USG auditors. Units are advised to begin planning how to implement documentation of their user access to systems with restricted or sensitive information or mission-critical systems on an annual basis.

For more information about the USG standard and UGA procedures, please contact Brian Rivers, Associate CIO for University Information Security, at brivers@uga.edu. For additional information about the USG standards, UGA procedures and documentation on EITS supporting resources, please visit <http://tinyurl.com/qhdwggk>.

If you want to be added to the automated listserv email to receive staffing change notifications, please contact EITS Access Services at adminfo@uga.edu or 706-542-4000, ext. 2.

**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 (UGANet)
Enterprise Information Technology Services (EITS-L)**



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.cits.uga.edu/vpit

February 14, 2014

MEMORANDUM

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

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

RE: USG User Account Standards, Follow-Up on Requirements

Last year, the University System of Georgia released new standards regarding user account management for information systems containing sensitive or restricted information, or other systems deemed as mission-critical to the University's ability to conduct business. These standards, which were effective July 1, 2013, were implemented at UGA through an automated process that disabled user's MyID or RACF ID when they left University employment. Through this implementation, units were also provided electronic notification of employees who depart the University, allowing them to meet these requirements. For background, information on these requirements is available at <http://ow.ly/kQnvX> on the Web.

In addition to requiring that institutions disable accounts for those departing employees within five (5) business days and adjusting user permissions appropriately for employees changing University roles within thirty (30) days, these standards also require a manual review of user access for these systems every four (4) months. A manual review of user access typically requires system support personnel to audit all user accounts for a system and verify with user departments that system access continues to be required for that employee to perform their duties. EITS Access Services has typically performed this audit of mainframe accounts every twelve (12) months.

Because UGA has taken steps to automate disabling of user accounts for departing employees, USG has provided UGA with an exception to the four-month user audit and will allow UGA to complete a user access audit each year for information systems containing sensitive or restricted information, or other systems deemed as mission-critical to the University's ability to conduct business.

User departments are expected to document compliance with these standards, which shall be subject to inspection by University or USG auditors. Units are advised to begin planning how to implement documentation of their user access to systems with restricted or sensitive information or mission-critical systems on an annual basis.

For more information about the USG standard and UGA procedures, please contact Brian Rivers, Associate CIO for University Information Security, at brivers@uga.edu. For additional information about the USG standards, UGA procedures and documentation on EITS supporting resources, please visit <http://tinyurl.com/qhdwggk>.

If you want to be added to the automated listserv email to receive staffing change notifications, please contact EITS Access Services at adminfo@uga.edu or 706-542-4000, ext. 2.

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 (UGANet)
Enterprise Information Technology Services (EITS-L)