ALL SITE ADMINISTRATORS/PRINCIPALS/APs: Review Requirements Of Authorization Reports
Category:

Audience: All Principals/APs

Due Date: n/a
Meeting Date: n/a

Attachment(s):   How_to_execute_and_print_PDF_and_Excel_Security_Roles_Report_from_SAP_portal.pdf

---

The purpose of this briefing is to inform administrators to perform the monthly reviews of the RACF Authorization and SAP Roles Reports.

M-DCPS utilizes a decentralized security model which requires a site administrator to determine appropriate authorizations and/or roles for their respective staff at his/her discretion. Access to RACF-related authorizations is controlled via Quad-A or the legacy CICS AAAA application, while SAP roles are controlled via the ERP Quad-A module.

Pursuant to Section 4.1.5 (Periodic Review of Systems Access by Site Supervisors) of the Network Security Standards, all site supervisors are **responsible for performing monthly reviews** of both the RACF Authorizations and SAP Roles Reports, and retaining these reports for a period of 12 months. In order to activate the print options for the SAP Roles report, select CTRL & P on your keyboard. A copy of the signed report must be available for auditors.

As a reminder, WGBM, WGBA, RSTR and PARS must be reviewed by the principal.

Parameters for WGBM and WGBA

- A maximum of 5 staff approvers may be granted access from the following groups: Principal, Assistant Principal, registrar of person identified as registrar, One primary Gradebook Manager or Attendance Manager, One Clerical selected by the Principal.
- Access must be limited to administrators, instructional or clerical personnel only.

Parameters for RACF

- ISIS/ACAD/TRACE-UPD is limited to Principal, AP and one other such as Registrar

Parameters for Payroll

- The Payroll Approval authorization can only be granted to Administrators

    o The person approving the payroll **MUST** be a District employee and they **MUST** be an **ADMINISTRATOR.**
    o Under **NO CIRCUMSTANCES** should any "role" in the payroll process (input or approval) be grated to anyone other than the District employee.

Individuals requiring additional assistance or who are experiencing technical issues in accessing or generating either report should submit a HEAT ticket via HSS (select "ASK ITS A QUESTION").

Contact: HEAT Self Service (http://selfservice.dadeschools.net) (n/a)
Department: Information Technology Services