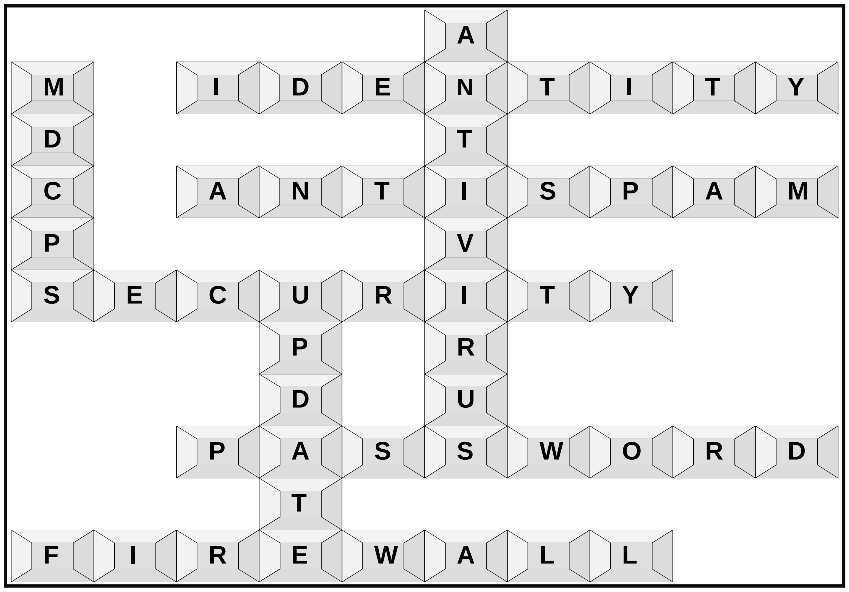
Internal Audit Report

Miami-Dade County Public Schools
Office of Management and Compliance Audits

ADMINISTRATIVE OFFICES NETWORK AND INFORMATION SECURITY AUDITS – HUMAN RESOURCES



Commendable efforts are being made to secure the information handled by the Human Resources department, but improvements are needed in specific areas.

December 2010

Mr. Jose F. Montes de Oca, CPA
Chief Auditor
Office of Management and Compliance Audits

Contributors to This Report:

Audit Performed by:
Mr. Luis Baluja
Ms. Dina Pearlman, CISA, CIA

Audit Reviewed by:
Mr. Jon Goodman, CPA
Mr. Trevor L. Williams, CPA

Supervised by:
Mr. Trevor L. Williams, CPA

Miami-Dade County Public Schools

giving our students the world

Superintendent of Schools
Alberto M. Carvalho

November 30, 2010

Members of The School Board of Miami-Dade County, Florida
Members of the School Board Audit Committee
Mr. Alberto M. Carvalho, Superintendent of Schools

Ladies and Gentlemen:

In accordance with the approved Audit Plan for the 2009-10 Fiscal Year, we have performed an audit of the Office of Human Resources, Recruiting and Performance Management information and network security.

Our audit concludes that, while commendable efforts are being made to secure the information handled by the department, improvements can be made in specific areas.

Our findings and recommendations were discussed with management. Their responses along with explanations are included herein. We would like to thank management for the cooperation and courtesies extended to our staff during the audit.

Sincerely,

José F. Montes de Oca

Jose F. Montes de Oca, CPA, Chief Auditor
Office of Management and Compliance Audits

TABLE OF CONTENTS

Page
Number

EXECUTIVE SUMMARY 1

INTERNAL CONTROLS 3

BACKGROUND 4

ORGANIZATIONAL CHART 6

OBJECTIVES, SCOPE AND METHODOLOGY 7

FINDINGS AND RECOMMENDATIONS:

1. Disaster Recovery and Environmental Issues In the Server Room 8

2. Cleansing of Information on Obsolete Computer Systems Not Adequately Documented 12

3. Administrative and Software Security Issues 14

4. Network Security Issues 17

MANAGEMENT'S RESPONSE 18

EXECUTIVE SUMMARY

The Human Resources (HR) office of Miami-Dade County Public Schools (M-DCPS) routinely handles highly sensitive and personal information about our employees – past, present, and potentially future. This information includes, but is not limited to: employment records, job appraisals, training and certification records, and health, benefits and financial records.

Our audit objectives were to assess the level of information security afforded to employees by HR. In order to best meet this objective, our audit covered the current network and information security practices in the division. It focused primarily on compliance with established M-DCPS Network Security Standards (NSS) and information technology (IT) best practices.

OVERVIEW OF FINDINGS

- A formal written departmental disaster recovery plan for restoration/recovery of legacy data in the case of catastrophic loss was needed in HR and was subsequently developed, but the plan should be tested periodically.
- Data back-ups of important source document and information are kept on-site instead of being sent to a remote location.
- Environmental conditions and support systems in the HR server room are less than optimal. The servers were subsequently moved to a secure and appropriate environment, but routine data back-up remains an issue.
- Written procedures requiring HR's staff to consistently document the cleansing of data from obsolete drives are needed and could strengthen controls over data management.
- Compliance with various Network Security Standards could be strengthened.
- Other network security issues not disclosed in this report to avoid compromising department data and IT resources were discussed with HR's administration. Some of these concerns were subsequently addressed and will be addressed to the extent resources allow.

Our findings indicate that HR administrators and staff take information security seriously. HR's management was prompt in correcting many of the issues we brought to their attention. However, in some cases not having full awareness of, or training with, current Network Security Standards and leading practices may have led to an increased risk of data compromise or loss.

It is important to note that IT security is a district-wide concern and while the findings and recommendations in this report are presented under HR, these conditions will necessitate global district-wide consideration. As such, the District's Information Technology Services department would need to be brought into discussions regarding possible solutions to address known and potential IT risks and exposures within M-DCPS' district offices.

Notwithstanding the risks potential that exist for certain equipment, data, and access controls, our audit did not disclose any serious data breaches originating from HR. However, the increasing risk of exposure and the vulnerability of data in today's environment make it incumbent upon the District to be increasingly more vigilant in protecting its employees' personal information. The findings and the seven (7) recommendations made in this report are intended to aid in this protection.

INTERNAL CONTROLS

The charts below summarize our overall assessment of the network and information security controls in place in the Office of Human Resources, Recruiting and Performance Management.

INTERNAL CONTROLS RATING			
CRITERIA	SATISFACTORY	NEEDS IMPROVEMENT	INADEQUATE
Process Controls		X	
Policy & Procedures Compliance		X	
Effect	X		
Information Risk		X	
External Risk[1]		X	

INTERNAL CONTROLS LEGEND			
CRITERIA	SATISFACTORY	NEEDS IMPROVEMENT	INADEQUATE
Process Controls	Effective	Opportunities exist to improve effectiveness.	Do not exist or are not reliable.
Policy & Procedures Compliance	In compliance	Non-Compliance Issues exist.	Non- compliance issues are pervasive, significant, or have severe consequences.
Effect	Not likely to impact operations or program outcomes.	Impact on outcomes contained.	Negative impact on outcomes.
Information Risk	Information systems are reliable.	Data systems are mostly accurate but can be improved.	Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions.
External Risk	None or low.	Potential for damage.	Severe risk of damage.

[1] The chart reflects the auditors' rating of internal controls for the various categories through the date of issuing the preliminary draft report; however, corrective actions taken by management, post-audit, appear to mitigate some external risks.

BACKGROUND

The Office of Human Resources, Recruiting and Performance Management (HR) comprises 14 departments (11 defined work locations) that provide a range of services including pre-employment screening and hiring, employment monitoring, and other employee services. The following is a brief synopsis of each department's functions:

> The Departments of Instructional Staffing and Non-Instructional Staffing screen, interview, and counsel prospective employees to maintain a pool of qualified applicants. The Certification department assists in facilitating proper licensure for employees through district and state issued certificates.
>
> Employment Standards performs work that is directly related to House Bill 1877, the Jessica Lunsford Act (JLA). Non-instructional personnel and contracted individuals must receive a Level II clearance, based on fingerprint results, as provided by the Florida Department of Law Enforcement (FDLE) and the Federal Bureau of Investigations (FBI). Fingerprint results are screened by the Fingerprinting Department and are subsequently submitted to the Office of Employment Standards for final review. Criminal histories are compared to the JLA Guidelines approved at the March 14, 2007, School Board Meeting. The clearance status of contracted personnel is provided to school sites and affected District Offices. This office also analyzes the results of the re-fingerprinting of current employees, as required by State Statute, for appropriate action.
>
> Personnel support programs provide prevention, intervention, and support services to employees. The Employee Assistance Program offers confidential help to employees who are experiencing problems on the job or at home. The Americans with Disabilities Act of 1990 (ADA) facilitates the District's compliance for affected employees.
>
> The Office of Civil Rights Compliance (CRC) mission is to deter and investigate harassment and discrimination based on protected categories. This mission is carried out through proactive training on discrimination, harassment, and cultural sensitivity as well as fair, impartial and timely investigation, and response to both internal and external complaints of illegal discrimination. CRC strives to ensure that all members of the Miami-Dade County Public Schools System value and respect each others'

contributions and opinions without regard to gender, race, social or ethnic background, or any of the protected categories.

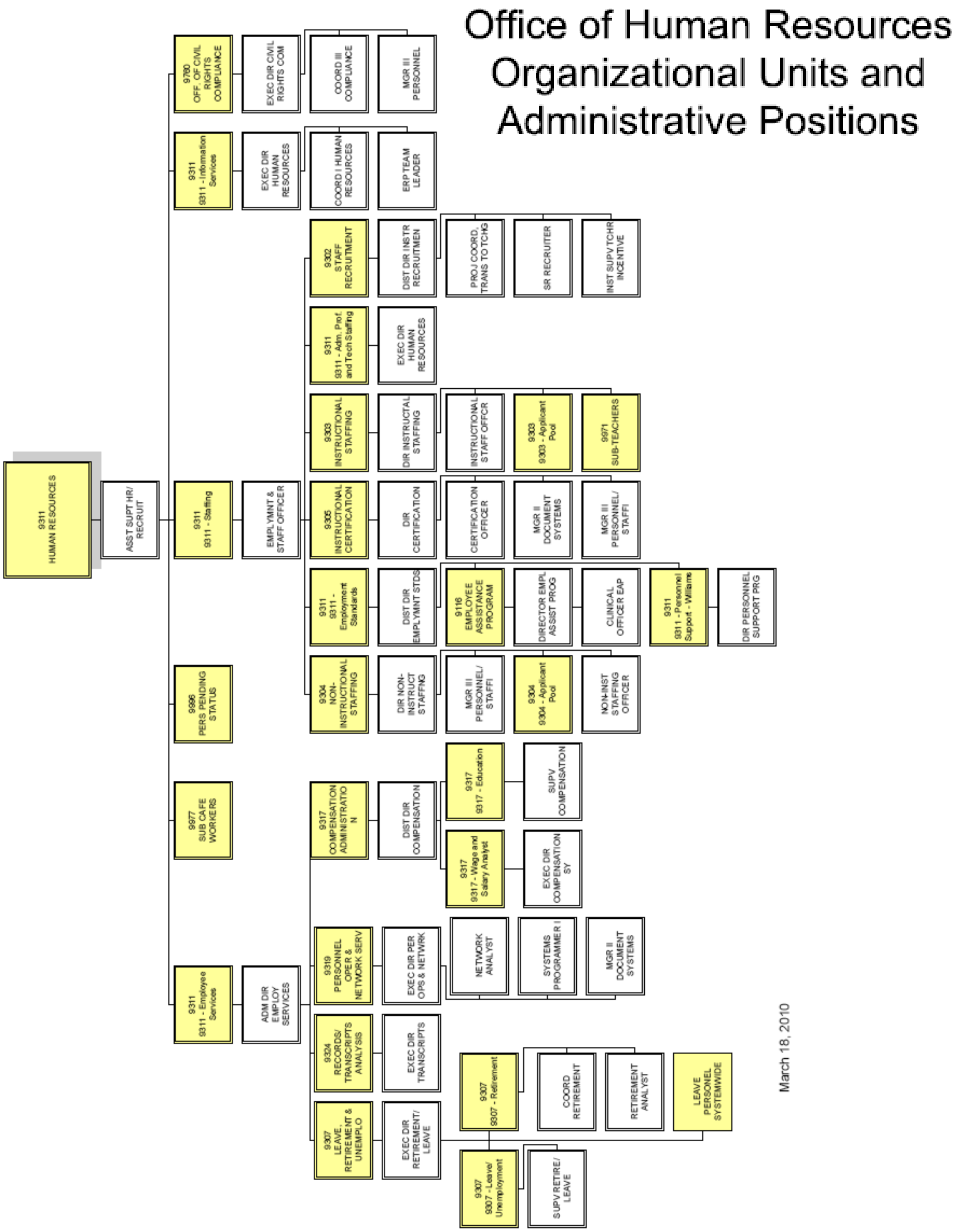
Compensation Administration has the responsibility for planning, developing and managing the District's various classification and compensation programs. The office administers the compensation provisions for five negotiated contracts and the compensation policies and procedures for five other employee groups on a timely basis.

Personnel Operations and Network Services manages the general drug screening of all applicants for full-time instructional and non-instructional positions, including administrative, charter schools, leased maintenance and temporary instructor positions. This office is also responsible for the completion of all Form I-9, Employment Eligibility Verification for new administrative, instructional, and non-instructional employees. In addition, this office is responsible for all operational functions as it relates to the Office of Human Resources including technical support to offices throughout the District with Personnel Reporting System (PERS). It operates and maintains the servers for the entire department and provides technical support to all HR work locations and computer equipment.

Personnel Records and Transcript Analysis provides employment and transcript verification and serves as custodian for all official personnel records of the District. Other responsibilities of this office include imaging of all HR files and handling subpoenas.

Leave, Retirement and Unemployment Compensation provides information for employees on the types of leaves of absence available to them and the eligibility criteria to take a leave. Information and counseling on the retirement plans and choices offered to employees by the Florida Retirement System is also provided. In addition, this department responds to unemployment compensation claims filed by M-DCPS' employees with the State of Florida.

The HR Information Services office serves as a conduit for the production of managerial reports and data queries within all areas and aspects of Human Resources. This office also includes e-Recruitment, organizational management for the SAP Enterprise Resource Planning (ERP) system and the creation of various monthly Board agenda items.



Office of Human Resources Organizational Units and Administrative Positions

9311 HUMAN RESOURCES
ASST SUPT HR/ RECRUIT
9780 OFF. OF CIVIL RIGHTS COMPLIANCE
EXEC DIR CIVIL RIGHTS COM
COORD III COMPLIANCE
MGR III PERSONNEL
9311 9311 - Information Services
EXEC DIR HUMAN RESOURCES
COORD I HUMAN RESOURCES
ERP TEAM LEADER
9311 9311 - Staffing
EMPLYMNT & STAFF OFFICER
9302 STAFF RECRUITMENT
DIST DIR INSTR RECRUITMEN
PROJ COORD, TRANS TO TCHG
SR RECRUITER
INST SUPV TCHR INCENTIVE
9311 9311 - Adm. Prof. and Tech Staffing
EXEC DIR HUMAN RESOURCES
9303 INSTRUCTIONAL STAFFING
DIR INSTRUCTAL STAFFING
INSTRUCTIONAL STAFF OFFCR
9303 9303 - Applicant Pool
9971 SUB-TEACHERS
9305 INSTRUCTIONAL CERTIFICATION
DIR CERTIFICATION
CERTIFICATION OFFICER
MGR II DOCUMENT SYSTEMS
MGR III PERSONNEL/ STAFFI
9311 9311 - Employment Standards
DIST DIR EMPLYMNT STDS
9116 EMPLOYEE ASSISTANCE PROGRAM
DIRECTOR EMPL ASSIST PROG
CLINICAL OFFICER EAP
9311 9311 - Personnel Support - Williams
DIR PERSONNEL SUPPORT PRG
9304 NON-INSTRUCTIONAL STAFFING
DIR NON-INSTRUCT STAFFING
MGR III PERSONNEL/ STAFFI
9304 9304 - Applicant Pool
NON-INST STAFFING OFFICER
9996 PERS PENDING STATUS
9977 SUB CAFE WORKERS
9311 9311 - Employee Services
ADM DIR EMPLOY SERVICES
9317 COMPENSATION ADMINISTRATION
DIST DIR COMPENSATION
9317 9317 - Education
SUPV COMPENSATION
9317 9317 - Wage and Salary Analyst
EXEC DIR COMPENSATION SY
9319 PERSONNEL OPER & NETWORK SERV
EXEC DIR PER OPS & NETWRK
NETWORK ANALYST
SYSTEMS PROGRAMMER I
MGR II DOCUMENT SYSTEMS
9324 RECORDS/ TRANSCRIPTS ANALYSIS
EXEC DIR TRANSCRIPTS
9307 LEAVE, RETIREMENT & UNEMPLO
EXEC DIR RETIREMENT/ LEAVE
9307 9307 - Retirement
COORD RETIREMENT
RETIREMENT ANALYST
LEAVE PERSONEL SYSTEMWIDE
9307 9307 - Leave/ Unemployment
SUPV RETIRE/ LEAVE

March 18, 2010

OBJECTIVES, SCOPE AND METHODOLOGY

In accordance with the approved Audit Plan for the 2009-10 Fiscal Year, we have performed an audit of the Office of Human Resources information and network security. The objectives of the audit were to determine whether adequate internal controls are in place to protect critical information and whether current District Network Security Standards are being adhered to. Our audit covers the current IT security practices in place in HR. We performed the following audit procedures to satisfy our audit objectives:

- Requested that each district department complete a site assessment survey and analyzed the survey results
- Interviewed District staff
- Examined and analyzed computer reports such as Resource Access Control Facility (RACF), Active Directory, and BigFix (District IT Management Tool)
- Examined and tested a random sample of servers and desktop computers for compliance to standards
- Inspected physical storage facility where servers are housed, and
- Performed various audit procedures as deemed necessary

We conducted this performance audit in accordance with generally accepted *Government Auditing Standards* issued by the Comptroller General of the United States of America. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions, based on our audit objectives. This audit included an assessment of applicable internal controls and compliance with the requirements of policies, procedures and rules to satisfy our audit objectives.

FINDINGS AND RECOMMENDATIONS:

1. DISASTER RECOVERY AND ENVIRONMENTAL ISSUES IN THE SERVER ROOM

According to the M-DCPS Network Security Standards (NSS), Section 4.1.1.7, *"Each department or school must maintain a disaster contingency plan to provide for recovery of data in case of catastrophic loss. At minimum, all MDCPS data must be backed-up once a week, and all mission-critical data must be backed-up daily. Data on the backup media will be verified as usable."*

1.1 A written departmental technology disaster recovery plan is not maintained by HR.

Our audit disclosed that although HR backs up information contained in its information system and the District's Information Technology Services Division (ITS) backs up the personnel master file data maintained on the District's mainframe, HR did not maintain a written disaster contingency plan for its department as required by the District's NSS. Consequently, an emergency restoration of important information contained in the HR servers would be difficult to achieve.

Technology disaster recovery plans such as the one called for in the District's NSS are intended to ensure continuity of services, and to lessen any adverse impact on operations in the event of a major disruption. A disaster recovery plan identifies and provides information on support resources needed, and the roles and responsibilities of those involved in the recovery process. Additionally, testing is essential to determine whether the plan functions as intended in an emergency situation, with the most useful conditions simulating a disaster to test overall service continuity.

Without a well designed plan, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied.

Subsequent to completing our fieldwork and issuing a draft report, HR management responsively drafted a disaster recovery plan for its servers, as recommended. The plan was submitted to ITS for their review and feedback and a copy was received by this office.

1.2 Backups of critical HR data are not being stored in an off-site location for data integrity and safety purposes as leading practices require.

Current IT leading practices include provisions for the secure storage, both on-site and off-site, of backed-up data files, software, and related documentation. As previously stated in Section 1.1 of this report, HR is backing up its data files and ITS is backing up the personnel master file data maintained on the District's mainframe. However, copies of HR data backup files have not been sent to an off-site location in the past one to two years. Prior to that, backups were being sent to the M-DCPS records retention vaults in West Miami-Dade County. ITS routinely backs up the servers under its care, both at the ITS secure site and at remote District locations. These backups are sent daily to a secure remote site in north Broward County. ITS currently does not provide this back-up service for the HR servers.

The School Board Administration Annex Building that houses HR servers is located on the west boundary of Miami-Dade County Emergency Management Storm Surge Evacuation Zone B. In the event of a major storm or other disaster, the building could be subject to flooding and/or wind damage, resulting in a loss of critical personnel data that the District is federally mandated to maintain. Maintaining backup files at a remote off-site location reduces the potential risks of loss of critical personnel data to the District.

Subsequent to completing our fieldwork and issuing a draft report, HR stated that it has re-instated the process of sending backups to the M-DCPS records retention vaults.

1.3 Servers are housed in a secure room but could be subject to harmful heat build-up in the event of an air conditioning failure.

The M-DCPS NSS 3.0 states: *"Adequate building security (both physical and environmental) must be provided for the protection of all physical and logical M-DCPS computer assets and especially sensitive applications and data. Security includes, but is not limited to, lockable doors and windows, limited access, protection from water and the elements, alarms, access controls, and surveillance devices such as cameras and monitors."*

Human Resources currently maintains 12 servers in a secure room in the School Board Administration Annex Building. Although these servers are physically secure, the environmental condition of the room is less than optimal for its application. For instance, a single supply vent from the building's air conditioning (AC) system, a wall-mounted auxiliary AC unit, and a supplemental floor fan are used to keep the room temperature at the required level. On the day the auditor visited the server room, the room temperature was cool but not cold. The room does not contain an alarm unit to warn of the failure or of the sudden increase in room temperature. Excessive heat could result in the failure of sensitive electronic equipment. It should be noted that in case of a building-wide power failure, the AC systems would be powered by the building's emergency generator.

We must note that Informational Technology Services (ITS) maintains a similar server room in School Board Administrative Building (SBAB). That room is equipped with a temperature alarm system, which is monitored 24 hours each day by Facilities Management security personnel, a back-up AC unit that automatically kicks in if the primary unit fails for any reason, and a halon fire suppression system. This is the type of protective arrangement that conforms to best practices.

Subsequent to the completion of our fieldwork and issuance of a draft report, all servers were physically moved to a server room in ITS main facilities, which has the necessary environmental and physical controls to protect the equipment and data, as recommended. Backing up the server data, however, continues to be the responsibility of HR staff rather than being included in the routine data back-ups performed by ITS. Please refer to Recommendation 1.2.

Recommendations:

1.1 Now that the Department of Human Resources have developed a disaster recovery plan that will enable it to timely resume processing in the event of a disaster, we recommend that the plan be also tested periodically to ensure it satisfies the Department's data recovery needs.

Responsible Department: **Human Resources**

Management's Response: A disaster plan is now in place with scheduled annual reviews.

1.2 Include HR servers in the routine data back-up and off-site storage functions performed by ITS.

Responsible Department: **Human Resources**

Management's Response: Daily backups of servers are currently taking place, with the data tapes being stored at an off-site location on a monthly basis. This process will continue to be performed by HR personnel.

2. CLEANSING OF INFORMATION ON OBSOLETE COMPUTER SYSTEMS NOT ADEQUATELY DOCUMENTED

The District's NSS (Section 4.1.2.13) state, *"Computers removed from service in the District must have the hard drives degaussed, re-formatted, or otherwise cleared of software and data before they can be sold, given away, or disposed of."*

2.1 Better recordkeeping is needed in order to Document Compliance with NSS 4.1.2.13.

HR Network Services indicated to us that it does have a policy for cleansing or re-imaging the hard drives of computers that it re-purposes. However, neither the policy nor the related processes are documented in writing. Staff from HR Network Services stated that when surplusing a computer, they check the computer, wipe or re-image the hard drives, salvage usable parts, and fill out an Outgoing Property Control Form. These forms are returned to the specific department within HR that previously owned the equipment. Records to verify the occurrence of this process are not maintained. Written procedures and full documentation promotes consistency in performing the stated surplus activities, thereby reducing the risk of confidential and sensitive information falling into the hands of unauthorized individuals.

Recommendation:

2.1 Develop written procedures to document the department's compliance with the District's NSS 4.1.2.13. Those written procedures should include maintaining a checklist and logs identifying the computers for which the hard drives were degaussed (demagnetized), re-formatted, or erased; the date of completing this action; the name of the person completing the action; and appropriately signed by employees, certifying that computer hard drives were sanitized.

Responsible Department: **Human Resources**

Management's Response: A data log has been established to properly document the cleansing and sanitization of all computers that are being surplus.

3. ADMINISTRATIVE AND SOFTWARE SECURITY ISSUES

There are a number of controls in place to assure security of M-DCPS processes. These include the Network Security Standards, State and Federal Statutes, and software controls built into the information systems. Departmental senior administrators are ultimately responsibility for enforcing these controls, granting access to sensitive data and programs, and informing authorized staff and users of these policies and staff's responsibilities.

3.1 Administrators did not regularly review and update Resource Access Control Facility (RACF) clearances.

The M-DCPS NSS 5.0.12 states: *"... site supervisors are required to review and retain a signed copy of the most recent RACF report showing that the authorizations held by site staff are appropriate, especially in regard to high risk authorizations..."*

During the initial stages of the audit, we requested copies of the signed monthly RACF report from HR administrators; however, those administrators were unable to provide us with the requested signed copies of the monthly RACF reports. Several administrators were unaware of which staff members had clearances for certain software packages. HR senior staff were very cooperative and willing to correct problems when they were made aware of them. In fact, the RACF reports were subsequently re-examined and most of the identified problems had been rectified.

3.2 An excessive number of employees had conflicting roles in the District's legacy mainframe payroll application, with the same employee having access to both RSTR (Payroll Approval) and PARS (Payroll Time Records) modules.

The segregation of work responsibilities is a fundamental control in preventing abuse and possible fraud. Without adequate segregation of duties and monitoring of role assignments for conflicts, the risk is increased that one person could circumvent internal controls. In the case of entering and approving the payroll, both the Network Security Standards (Section 4.1.4.1) and the Payroll

Processing Procedures Manual (Chapter 3) mandate strict limits on the quantity, job roles, and administrative levels of authorized personnel.

Our audit found 10 RSTR/PARS conflicts in six of the 11 departments within HR. Four departments were not in compliance with RSTR access; four departments had multiple individuals with access to both applications; and three departments had an excessive number of individuals with access to these applications. Although the mainframe payroll software has certain controls embedded, the large number of individuals with dual access increases the risk that those controls can be circumvented through collusion involving two or more employees. HR eliminated nine of the noted role conflicts after we brought this matter to their attention. One department in HR still has two administrators with access to both RSTR and PARS.

Due to programmatic limitations with the legacy mainframe software, the Senior Administrator of each work location needs to have clearance to both the Payroll Time Records – PARS and Payroll Approval – RSTR applications in order to grant access to their employees. This is a level of risk that the District has accepted. However, as previously stated, there are software controls embedded in the program that prevent a single individual from both entering and approving the same payroll information. Management asserts that this dual-access issue will be eliminated upon full cut-over to SAP.

3.3 Screensaver timeouts are not consistently used.

The M-DCPS NSS 4.1.1.10 states: *"All administrative computers and server consoles that are used to access or control sensitive data must have a screen saver timeout and password after a specific period of inactivity or some other lockout mechanism to prevent unauthorized persons from accessing the data via the logged-in user's account. The Windows timeout with password is available even if the specific application does not have one. Users should also be in the habit of locking their computer or logging off when they are finished or leaving the computer unattended, even for a brief time."*

We observed and physically checked a sample of the HR's computers and found inconsistent application of screensaver timeout required by the NSS.

Recommendations:

3.1 Monitor the RACF reports as required by M-DCPS NSS 5.0.12 and modify accesses as appropriate.

Responsibility Department: Human Resources

Management's Response: All department administrators routinely review staff access and modify SAP and Mainframe access as needed.

3.2 Periodically review the job functions of staff members and grant access to only those programs required by their current duties, giving care to avoid granting access to incompatible operations.

Responsibility Department: Human Resources

Management's Response: Only the Senior Administrator responsible for delegating access to RSTR and PARS has access to both applications.

3.3 Require all appropriate staff to comply with NSS 4.1.1.10 by using screensaver timeouts and by properly locking their computer when they are away from their desks.

Responsibility Department: Human Resources

Management's Response: A group policy has been implemented to change the screen saver settings to all of the computers within HR.

4. NETWORK SECURITY ISSUES

Security controls are intended to protect the integrity, confidentiality, and availability of data, IT resources, and sensitive information. Without adequate security and application and network controls, the integrity, confidentiality, and availability of data and IT resources could be compromised, increasing the risk that department data and IT resources may be subject to improper disclosure, destruction, or modification. During our audit, we identified certain network security controls in addition to those reported elsewhere in this report that need improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising the department's data and IT resources. However, appropriate department staff have been notified of these issues.

Subsequent to discussing these matters with management and issuing our draft report, management took measures to address some of these concerns and has indicated that they will address the remainder to extent that resources allow them to.

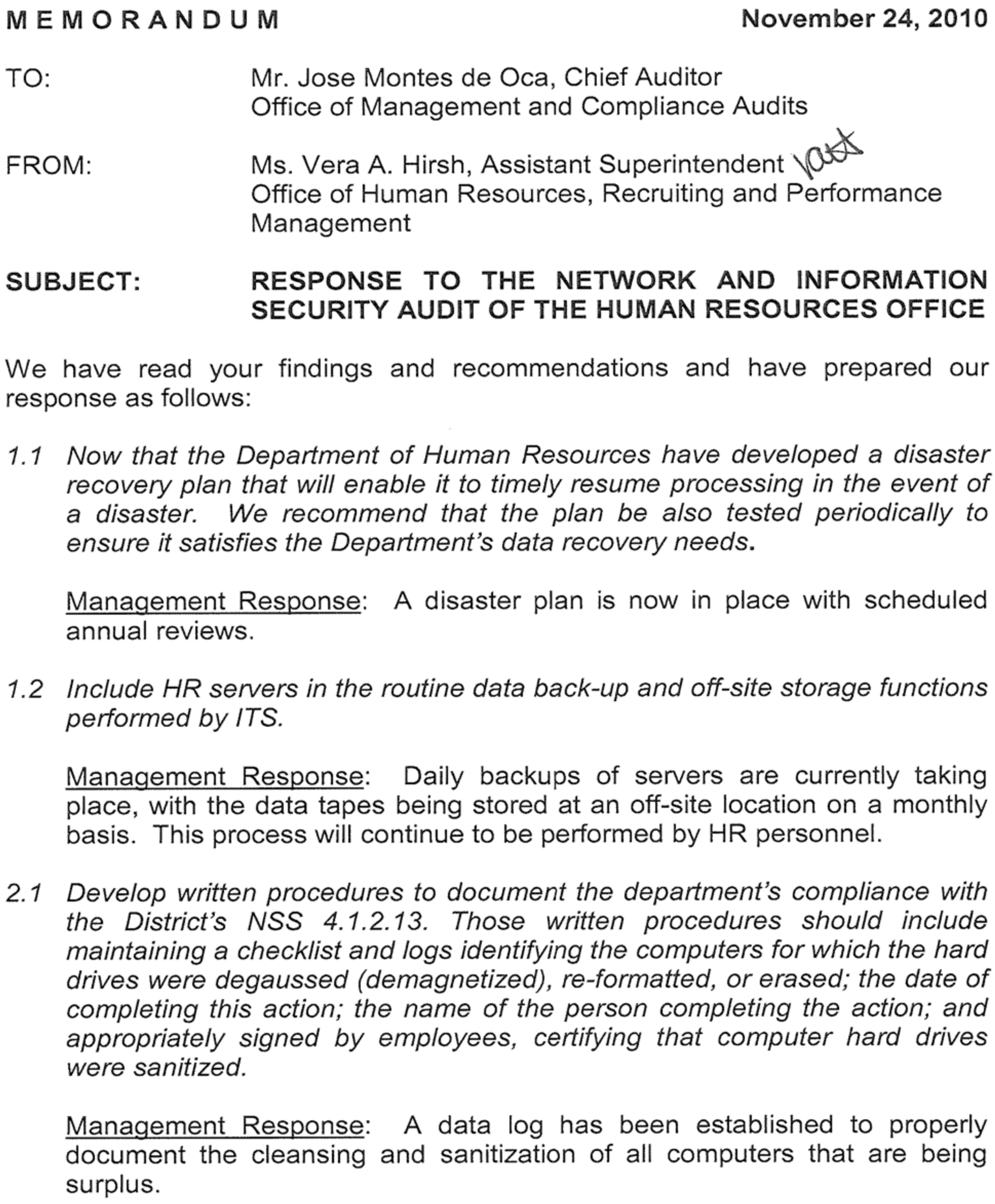
Recommendation:

4.1 The Department should implement the appropriate network controls over the department's data and IT resources.

Responsibility Department: **Human Resources**

Management's Response: All network issues identified by the auditor have been addressed and resolved in order to maintain the integrity and confidentiality of the files and systems.

MANAGEMENT’S RESPONSE



M E M O R A N D U M **November 24, 2010**

TO: Mr. Jose Montes de Oca, Chief Auditor
Office of Management and Compliance Audits

FROM: Ms. Vera A. Hirsh, Assistant Superintendent
Office of Human Resources, Recruiting and Performance Management

SUBJECT: RESPONSE TO THE NETWORK AND INFORMATION SECURITY AUDIT OF THE HUMAN RESOURCES OFFICE

We have read your findings and recommendations and have prepared our response as follows:

1.1 Now that the Department of Human Resources have developed a disaster recovery plan that will enable it to timely resume processing in the event of a disaster. We recommend that the plan be also tested periodically to ensure it satisfies the Department's data recovery needs.

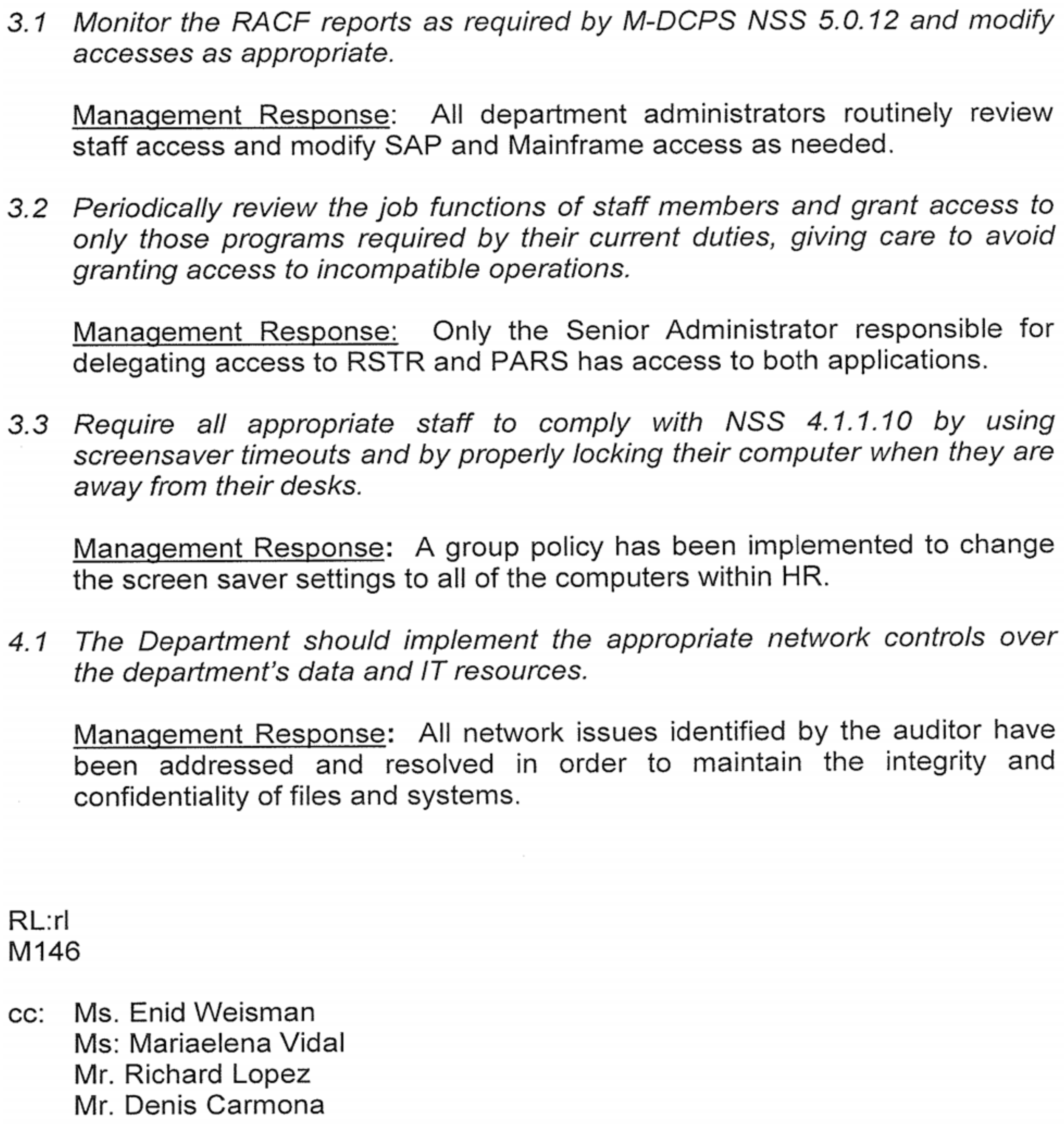
Management Response: A disaster plan is now in place with scheduled annual reviews.

1.2 Include HR servers in the routine data back-up and off-site storage functions performed by ITS.

Management Response: Daily backups of servers are currently taking place, with the data tapes being stored at an off-site location on a monthly basis. This process will continue to be performed by HR personnel.

2.1 Develop written procedures to document the department's compliance with the District's NSS 4.1.2.13. Those written procedures should include maintaining a checklist and logs identifying the computers for which the hard drives were degaussed (demagnetized), re-formatted, or erased; the date of completing this action; the name of the person completing the action; and appropriately signed by employees, certifying that computer hard drives were sanitized.

Management Response: A data log has been established to properly document the cleansing and sanitization of all computers that are being surplus.



3.1 *Monitor the RACF reports as required by M-DCPS NSS 5.0.12 and modify accesses as appropriate.*

Management Response: All department administrators routinely review staff access and modify SAP and Mainframe access as needed.

3.2 *Periodically review the job functions of staff members and grant access to only those programs required by their current duties, giving care to avoid granting access to incompatible operations.*

Management Response: Only the Senior Administrator responsible for delegating access to RSTR and PARS has access to both applications.

3.3 *Require all appropriate staff to comply with NSS 4.1.1.10 by using screensaver timeouts and by properly locking their computer when they are away from their desks.*

Management Response**:** A group policy has been implemented to change the screen saver settings to all of the computers within HR.

4.1 *The Department should implement the appropriate network controls over the department's data and IT resources.*

Management Response**:** All network issues identified by the auditor have been addressed and resolved in order to maintain the integrity and confidentiality of files and systems.

RL:rl
M146

cc: Ms. Enid Weisman
Ms: Mariaelena Vidal
Mr. Richard Lopez
Mr. Denis Carmona

The School Board of Miami-Dade County, Florida, adheres to a policy of nondiscrimination in employment and educational programs/activities and programs/activities receiving Federal financial assistance from the Department of Education, and strives affirmatively to provide equal opportunity for all as required by:

Title VI of the Civil Rights Act of 1964 - prohibits discrimination on the basis of race, color, religion, or national origin.

Title VII of the Civil Rights Act of 1964, as amended - prohibits discrimination in employment on the basis of race, color, religion, gender, or national origin.

Title IX of the Education Amendments of 1972 - prohibits discrimination on the basis of gender.

Age Discrimination in Employment Act of 1967 (ADEA), as amended - prohibits discrimination on the basis of age with respect to individuals who are at least 40.

The Equal Pay Act of 1963, as amended - prohibits sex discrimination in payment of wages to women and men performing substantially equal work in the same establishment.

Section 504 of the Rehabilitation Act of 1973 - prohibits discrimination against the disabled.

Americans with Disabilities Act of 1990 (ADA) - prohibits discrimination against individuals with disabilities in employment, public service, public accommodations and telecommunications.

The Family and Medical Leave Act of 1993 (FMLA) - requires covered employers to provide up to 12 weeks of unpaid, job-protected leave to "eligible" employees for certain family and medical reasons.

The Pregnancy Discrimination Act of 1978 - prohibits discrimination in employment on the basis of pregnancy, childbirth, or related medical conditions.

Florida Educational Equity Act (FEEA) - prohibits discrimination on the basis of race, gender, national origin, marital status, or handicap against a student or employee.

Florida Civil Rights Act of 1992 - secures for all individuals within the state freedom from discrimination because of race, color, religion, sex, national origin, age, handicap, or marital status.

School Board Rules 6Gx13- 4A-1.01, 6Gx13- 4A-1.32, and 6Gx13- 5D-1.10 - prohibit harassment and/or discrimination against a student or employee on the basis of gender, race, color, religion, ethnic or national origin, political beliefs, marital status, age, sexual orientation, social and family background, linguistic preference, pregnancy, or disability.

Veterans are provided re-employment rights in accordance with P.L. 93-508 (Federal Law) and Section 295.07 (Florida Statutes), which stipulate categorical preferences for employment.

Revised 5/9/03

INTERNAL AUDIT REPORT

Administrative Offices Network and Information Security Audits – Human Resources

MIAMI-DADE COUNTY PUBLIC SCHOOLS
Office of Management and Compliance Audits
1450 N.E. 2nd Avenue, Room 415
Miami, Florida 33132
Telephone: (305)995-1318 ♦ Fax: (305)995-1331