MIAMI-DADE COUNTY, FLORIDA

MIAMI INTERNATIONAL AIRPORT

MIAMI-DADE COUNTY

Miami Dade Aviation Department
P.O. Box 526624
Miami, Fl 33152-6624
http://www.miami-airport.com

Departmental Standard Operating Procedure (DSOP)
DSOP No. 02-03
Last Amended: 4-23-12
Effective: 4-24-14

SUBJECT: COMPUTER RESOURCES AND TELECOMMUNICATION SYSTEMS

PURPOSE: To establish policies and guidelines for the proper utilization of departmental computers, data processing, and telecommunication resources.

I. BACKGROUND:

The Miami-Dade Aviation Department (MDAD) relies on its computer network and its telecommunication systems to conduct its business. It is the duty of every employee to use departmental computers and telecommunication resources responsibly, professionally, ethically, and lawfully. Computer and telecommunication resources include, but are not limited to: host computers, file servers, application servers, communication servers, mail servers, fax servers, web servers, workstations, stand-alone personal computers (PC), laptops, software, data files, all internal and external computer communications networks, telephones, cellular phones, smartphones, portable storage devices, and telecommunication voice and data equipment.

II. AUTHORITY:

A. Chapter 274 of the Florida Statutes, Tangible Personal Property Owned by Local Governments.
B. Chapter 119 of the Florida Statutes, Public Records.
C. Chapter 25 of the Miami-Dade County Code, Miami-Dade Aviation Department Rules and Regulations.
D. Operational Directive No. 99-02, Miami-Dade Aviation Department Operational Directives.
E. Operational Directive No. 99-03, Miami-Dade Aviation Department Written Directive System.
F. Departmental Standard Operating Procedure No. 00-01, Miami-Dade Aviation Department Departmental Standard Operating Procedures.
G. Miami-Dade County Administrative Order No. 5-5, Acquisition, Assignment and Use of Telecommunication Devices and Network Resources.
H. Miami-Dade County Administrative Order No. 8.2, Use, Care, Control, and Disposal of County Property.
I. Miami-Dade County Implementing Order No. 6-8, Use of Cellular Telephone and Similar Wireless Devices while Operating County Vehicles.

J. Miami-Dade County Leave Manual, Section 11.04.02, Bereavement Leave: Authorized Use.
K. Miami Dade County's Social Media Policies, which are available at http://intra.miamidade.gov/policies/library/social-media-guidelines.pdf

III. DEFINITIONS:

A. *Computer Resources:* All hardware, software, maintenance agreements, personnel, and procedures that are part of data processing solutions.
B. *Department:* The Miami-Dade Aviation Department.
C. *Freeware:* Computer software that is downloaded for free from the internet.
D. *Hardware:* Computers and computer-related equipment and devices such as controllers, terminals, scanners, workstations, printers, file servers, routers, switches, cellular telephones, pagers and other wireless devices.
E. *ISTD:* Information Systems and Telecommunications Division.
F. *I.T. Service Desk/NOC:* Network Operations Center. Also referred to as Help Desk.
G. *Network:* Series of computers or devices interconnected to allow users to share information and resources.
H. *Postmaster:* Term used to identify the administrative email account used to distribute and forward mass emails in a network.
I. *Shareware:* Computer software that is distributed for free on a trial basis. The trial period and functionality vary dependent on the author.
J. *Software:* Computer programs and procedures that enable the computer to perform predetermined functions, and can usually be altered by a computer programmer.
K. *Telecommunications:* Any form of information handling in which a data processing or voice system utilizes communication facilities.
L. *User:* Any person, group of persons, or organization using County telephone services, computer resources or benefiting from the data processing services provided.

IV. POLICY:

A. This procedure has been developed to ensure that computer resources and telecommunication systems, inclusive of the Internet and email, are to be used for the benefit and in the best interest of the County and the Department. ISTD will monitor usage of electronic equipment, files, documents, Internet and Intranet activity, and email services based upon the importance of data protection, information privacy and network security.

B. All information is subject to Chapter 119 of the Florida Statutes concerning public records, which makes every record public unless there is a specific exemption approved by the State Legislature.

C. Users of the Department's computer resources and telecommunications systems understand and agree to this DSOP without exception. Users acknowledge their agreement with the Computer Use Policy (Exhibit A), which is displayed just before logging into the Department's computer network.

D. The County has implemented tools that prevent employees from using the County network to access internet sites that are considered unacceptable for County business. Attempts to access websites that are considered unacceptable for County business will be logged and reported to the respective Assistant Director.

E. The use of departmental computer resources and telecommunications systems is a privilege that may be revoked at any time. Violations will be taken seriously and may result in disciplinary action, including possible termination of employment, as well as civil and/or criminal liability.

F. The Department has established a uniform policy and procedure regarding the use of electronic mail for bulk distribution and sending of mass messages. The policy is intended to reduce junk mail and to avoid unnecessary traffic on the Department's email servers.

G. Aviation Department employees will refrain from using wireless telecommunication devices while driving a county vehicle, unless a hands free device is utilized. Wireless telecommunication devices include cellular phones, tablet computers, radios, pagers, laptops, and anything else that can lead to the distraction of operating a vehicle. Unauthorized use of wireless devices or misuse of wireless telecommunication devices shall result in disciplinary action as outlined in Implementing Order 6-8, Use of Cellular Telephones and Similar Wireless Devices While Operating County Vehicles.

V. PROCEDURES:

A. Computer Hardware, Systems, Radios, Pagers, Telephones, Laptops, Smartphones and Cellular Telephones.

1. Proper Use:

a. Maintain the integrity of Personal Computers (PCs), hardware peripherals, and telephone equipment by not exposing them to potential damage from debris, spills, or other physical damage.
b. Report damage or theft of all computer and telecommunication equipment to ISTD. A police report will be needed if Department equipment is stolen or cannot be located.

2. Prohibited Use:

a. Accessing the Department network, or using workstations, smartphones, Departmental hardware, software, peripherals, and telecommunications equipment for non-departmental business purposes.
b. Creating, storing, displaying, posting or distributing obscene or slanderous material.
c. Making personal calls on County long distance telephone lines or dialing 411 to obtain telephone numbers listed in the telephone book, or available on the internet.

d. Employees are prohibited from making personal long distance calls that incur a charge to the County, whether domestic or international, using County owned communication devices.

3. Use of Cellular Telephone While Driving

a. The Department is fully committed to the highest standard of safety, and drivers are required to provide full attention to safe, smooth and efficient operation of County owned equipment. Failure to comply with this policy will result in progressive disciplinary action in accordance to Miami-Dade County personnel rules and regulations.
   i. Proper Use:
      a) Cellular telephones are only to be used when an immediate need exists to make or receive a call.
      b) Aviation employees will refrain from using any wireless telecommunication device while driving a County vehicle, unless a hands free device is utilized.
      c) If it becomes absolutely necessary to use a cellular phone while driving, employees are expected to pull off the roadway and park before making or answering a call.
   ii. Prohibited Use:
      a) Making and/or receiving calls without a hands free device (earpiece, Bluetooth, etc.) while driving a County vehicle.
      b) Texting while driving a County vehicle.
      c) Uploading/downloading data or music.
      d) Surfing the web or playing electronic games on a County issued cell phone or device.
      e) Taking non-work related photos or video recording on a County issued cell phone or device.

4. Pager and Radio Usage

a. The Department issues two-way radio communication devices, which include Motorola 400 MHz, GE 800 MHz and Ground Control Radios exclusively.
b. Radios must only be used for County business.
c. Each division is responsible for maintaining pager and radio inventories.
d. Division employees, who are no longer required to use a County-issued pager or radio in their professional capacity, must relinquish their device. The unit should be removed the Division's inventory and the ISTD Radio Shop should be contacted at 305-869-4023.
e. Technical problems experienced with Department issued two-way radios, or any related peripherals should be reported to the ISTD Help Desk at extension 5900.

5. Requests for Pagers, Computers, Radios, Telephones, Cellular Phones and Network Services:

a. ISTD, together with the Administrative Services Division, will coordinate the addition, deletion and modification of accounts for new hires, transfers and terminations. When it is necessary to terminate an account, it will be disabled and group memberships will be discontinued.
   i. After 30 days the mailbox and home directory will be archived, and the account becomes inactive.
   ii. After 90 days the account is deleted.
b. County issued pagers, computers, radios, telephones, cellular phones, and smartphones are property of Miami-Dade County and are to be used primarily for conducting official County business.
c. To establish or change service The Request for Telecommunications Service Form (see Exhibit B) should be completed. It can be downloaded at: http://mdad-intranet/MDAD_Forms/ISD_Forms/isd_forms.html.

6. Procedures for Reporting Computer Related Problems to ISTD:

a. The Help Desk, extension 5900, should be used to report problems related to all computer devices, software and network issues, radios and other telecommunications devices. The Help desk can be reached from external locations at 305-869-5900.
b. The Help desk operates 24 hours a day, seven days a week.
c. Callers should clearly identify their problem when calling; state how it occurred, or the application being used at the time. If an error message appears on the screen, either write down the message or obtain a screen print to relay the information to the Help Desk staff or the technician assigned to troubleshoot the problem.
d. The problem call will be logged, and a numbered ticket will be initiated. Callers should use this number to inquire about the status of their problem ticket.
e. The problem ticket will be assigned to a technician, who will contact the caller within 24 hours (holidays and weekends excluded). Open tickets are monitored through resolution.
f. After the problem has been fixed, an online survey will be sent out via email to obtain feedback on the quality of the service provided.

7. Software Licensing and Copyright Laws:

a. The software installed on a departmental PC has been licensed to ISTD for use on a single computer. Duplication and distribution constitutes a copyright violation and is strictly prohibited.
b. A request for software that is available as a trial, as freeware, or as shareware will be handled as a request for the licensed version. After the approved request has been submitted, ISTD will complete an assessment. If

the software meets the needs of the requestor and the Department, it will be installed on the computer for the trial. The fully licensed version will be procured by ISTD before the trial expires if the requestor acknowledges that the software will be used after the trial.

c. ISTD staff will conduct periodic random desktop and system audits to validate licensing. Violations will be reported to the appropriate Division Manager and Assistant Director.
d. Unauthorized software will be removed to prevent infringement of copyrights. Possession of a personal license for a software product does not cover the Department and could constitute a violation of copyright laws. This includes the installation of games and screen savers.

8. Network Access

a. A Network Account Request Form (Exhibit C) should be completed to initially request network access for a new employee.
    i. The form can be downloaded on the intranet at: http://mdad-intranet/MDAD_Forms/ISD_Forms/isd_forms.html.
b. A Request for Service Form (Exhibit D) should be completed to establish, upgrade, or relocate a workstation; request network applications or other specialized PC software; and request other hardware.
    i. The form can be downloaded at: http://mdad-intranet/mdad_Forms/ISD_Request_Form.PDF.
c. Creation and changing of passwords:
    i. All network accounts and passwords are for the exclusive use of the individual for whom they were created, and must be used in a manner consistent with the business of the Department.
    ii. Employees should use different passwords for different accounts and applications.
    iii. For the ideal password, use a strong password that meets the following guidelines:
        a) It will consist of seven to fourteen characters. For Security reasons, fourteen characters are preferable.
        b) It will contain both uppercase and lower case letters.
        c) It will contain numbers.
        d) It will contain symbols such as: ‘ ! “ ? $ % ^ & * ( ) _ - + = { [}] : ; @ ` ~ # | \ < ,>. /
        e) It will contain a symbol in the second, third, fourth, fifth, or sixth position (for encryption purposes).
        f) It will not resemble any of your previous passwords.
        g) It will not be your name, your friend’s name, the name of a family member or your login.
        h) It will not be a dictionary word or a common name.
    iv. Employees will be required to change their password frequently, at least every six weeks.

v. Disclosing passwords is prohibited. If during an emergency a password is disclosed it should be changed immediately.

d. Prohibited Activities:
   i. Emailing passwords to others.
   ii. Using the network for mass electronic mailings ("spamming"), chain messages, transmitting unsolicited material, or advertising for personal purposes.
   iii. Circumventing established security procedures, or not reporting the known attempts by internal or external entities.
   iv. Altering or copying a file belonging to another user, without first obtaining permission.
   v. Connecting to other computer systems for unauthorized access.
   vi. Introducing viruses into the Department's network.
   vii. A request to reset a password by anyone other than the network account owner is prohibited.

9. Email and Network Usage

a. Proper Use of email:
   i. Include only intended parties in an email.
   ii. When responding to a person's question on a mailing list, send the response to the individual, unless all recipients on the list would clearly benefit from the response.
   iii. Remove personal and transitory messages from the inbox on a regular basis to avoid wasting storage space.
   iv. Include your business information at the bottom of email messages when communicating with people who may not know you. This should include your name, telephone number, position, organization, email address, and any relevant disclaimer.

b. Prohibited Activities:
   i. Sending global messages by bypassing the Postmaster email procedures.
   ii. Transmitting emails that could make the County liable to a charge of illegal discrimination, copyright violation, negligence, or false advertising.
   iii. Transmitting emails containing information of partisan political activities.
   iv. Fundraising emails, except for County or Department approved activities, such as the County's United Way Campaign.
   v. Exposure of information which management considers sensitive or confidential, such as SSI (Sensitive Security Information), or information that the sender is not authorized to release.
   vi. Emails intended to harass or annoy.
   vii. Obscuring one's identity by falsifying one's network address or name.
   viii. Damaging or deleting another user's files without authorization.

ix. Attempting to circumvent security restrictions, except when sanctioned by management in order to test security.
x. Modifying server or network configurations without management approval.
xi. Originating or propagating chain letters.
xii. Using software that has not been previously tested and approved by ISTD.
xiii. Using email or the internet to make official commitments on behalf of the Department, or another County Department, without proper authorization.
xiv. Representing oneself as a spokesperson for the Department, or another County department without Departmental authorization.
xv. Disclosing the contents of email messages for the sole purpose of embarrassing the sender, or satisfying idle curiosity about the affairs of others.

c. PostMaster Email Messages:
i. PostMaster email messages should be used to communicate events affecting employees, the operations of the airport, health and safety issues, or emergencies which have a local or regional impact and need to be communicated quickly.
ii. Approved categories include: messages related to the department's written directives, to include departmental standard operating procedures (DSOP), standard operating procedures (SOP), operating directives (OD), MDX advisories, open enrollment and employee benefit notifications, employment opportunities, deaths (as outlined in section 11.04.02 of the Miami-Dade County Leave Manual), inoperable cellular devices for Chiefs and above, Information Technology announcements or outages, major events or directives from the Mayor (or designee), major events or directives from the Aviation Director (or designee), hurricane advisories, security announcements and Be On the Look Out (BOLO) bulletins.
iii. All PostMaster email messages must be sent via the Postmaster account with the exception of Emergencies and Hurricane advisories. These advisories may be sent out directly by the Deputy Director(s), Assistant Directors, or authorized designee.
iv. Departmental announcements to be sent via PostMaster must be sent by, or copied to the applicable Division Director, and will only be sent once. Messages will be set to expire after event has passed.
v. ISTD staff, or authorized designee, will be the administrator of the PostMaster account with the ability to send PostMaster messages.
vi. Employees may not use the Department's computer systems for the transmission of any type of unsolicited bulk electronic mail advertisements or commercial messages that are not Department and/or Miami-Dade County related.
vii. Items not approved for global circulation via the PostMaster account will be published on the MDAD Intranet.

a) Items for the MDAD Intranet include: Messages about retirements, special events, fundraisers, restaurant specials, articles, earned leave requests, discounts, airport related news features, What's New, thank-you messages and Out of Office Messages for Chiefs and above.
b) The MDAD United Way Coordinator must approve all United Way communications before they are published.
c) Out-of-the-office messages will be published on MDAD's Intranet for Chiefs and above when that person will be out of the office for a period of one week or more. The out-of-office automatic reply within Outlook should be used in other instances.
d) Items intended to be published on the Intranet must be forwarded to ISTD via the CompRoom account. These items will be forwarded to the Terminal Operations Division for posting.

viii. Political endorsements, political propaganda or messages of a religious nature are not approved for distribution to MDAD users.

d. Procedures For Sending Emails via PostMaster
i. Email messages intended to be sent via PostMaster must be forwarded to ISTD in its final format, to the CompRoom account. No editing will be done by ISTD staff.
ii. Announcements to be circulated via PostMaster must either originate from or copy a Division Director (or designee).
iii. The Originator of the email message is responsible for the format and content of the email message, the attachment, and the subject line.
a) The subject line should briefly and clearly summarize the email message.
1. Example:

Instead of	Subject: Out of Office
Use	Subject: Out of Office – John Smith

iv. Acceptable file types include: Word, Excel, PowerPoint and PDF.
v. The contact person and telephone number must be included on all PostMaster messages.
vi. All attachments pertaining to the message must be included with the message.
vii. All PostMaster messages with attachments will be sent as a link to a file on an internal server.
viii. Messages can be sent to either or both mass distribution lists, the Originator must specify which group(s) to send to.
a) Aviation Department users - all Department employees and contracted workers functioning as Department employees.
b) Other Users – Non Departmental users employed at the Airport.

ix. PostMaster messages must have a cohesive and consistent MDAD brand image. No image, other than the approved MIA co-branded logo (Exhibit E), may be used in the message body.
x. ISTD will determine if the information is appropriate to be distributed via PostMaster.
xi. To help protect the Department from cyber security threats, certain links are blocked by the Department's security filters. ISTD will confirm that the links included in the PostMaster messages can be viewed by all recipients in the mass distribution lists. If links are not in the permitted links category, the Originator of the PostMaster message will be notified that the message cannot be sent.

e. Unauthorized Access to Internet Sites
i. It is the intent of ISTD to prevent improper or unauthorized access to Internet sites.
ii. Users should be aware that ISTD will randomly monitor sites being viewed by employees at any time.
iii. Employees are strictly prohibited from accessing sites that contain material of an adult or pornographic nature.

f. Intranet and Internet Access
i. The Department's intranet was created to provide valuable information to employees throughout the Aviation Department. It is also a vehicle for sharing information among divisions, and for providing static information and forms.
a) Intranet site: http://mdad-intranet.
ii. The Department's external site is available to the public, and can be accessed at: http://www.miami-airport.com.
iii. Users who encounter problems accessing the Internet or the Intranet should contact the Help desk at extension 5900.
iv. Procedures for posting and updating information to the Department's intranet and internet sites:
a) Public and Customer Relations is the Administrator of the intranet/internet websites and web content.
b) Community Information and Outreach (CIAO) hosts the internet site and in partnership with the Department, supports the technical aspects.
c) Requests for content changes should be directed to Public and Customer Relations/Creative Services via email:webrequests@miami-airport.com.
d) The Intranet web-site will be updated on an as-needed basis, with the exception of time-sensitive information requiring immediate posting.

10. Department Network Access from Mobile Devices

a. Once connected to the Departmental Network, personal mobile devices and tablets must adhere to Miami-Dade County Administrative Order No. 5-5,

Acquisition, Assignment and Use of Telecommunication Devices and Network Resources.

b. Departmental employees that have agreed to the Terms and Conditions for Mobile Devices (Exhibit F) can be connected to the Departmental Network and have access to Departmental Email services on their personal mobile device.
c. It is the responsibility of the user to be accountable for personal devices connected to the Department's network or email accounts by immediately contacting ISTD to report if the device is lost, damaged, or no longer in your possession.
d. If using a personally owned mobile device, the Department is not responsible for any related costs from the user's service provider.
e. Information stored on your personal device may be requested pursuant to Chapter 119 of the Florida Statutes, Public Records.
    i. All information stored on the device, including, but not limited to email messages and websites accessed, is subject to public records disclosure, and with limited exceptions, is not exempt from such disclosure.
f. For security protection, the device should be configured to include the following:
    i. Password timeout with lock.
    ii. If the device is misplaced, stolen or reassigned it may be reset to factory settings.

11. Registration and Cancellation Procedures for Departmental Training

a. An announcement of the monthly training schedule is sent out via email (PostMaster), and updated on the Departmental Intranet site. The registration form, which is available on the Intranet site, should be attached to an email to register for a class.
b. In the event an employee cannot attend a training course previously registered for, the Division may send someone else from the same Section/Division as a replacement. Please note that cancellations must be made 48 hours in advance. Divisions will be charged for "no shows" and last minute cancellations. The Training Coordinator should be notified of any enrollment changes.
c. Completing a particular course does not automatically guarantee the employee will receive the software or an upgrade.
d. Training for telephone system usage is to be scheduled at the request of a Division Manager. A Request for Telecommunications Service Form (Exhibit B) should be forwarded to the ISTD Telecommunications Section for processing.

12. Disposal of Computer Equipment

a. Users must adhere to County A.O. 8.2, Use, Care, Control, and Disposal of County Property, regarding the use, liabilities, and responsibilities regarding County equipment. (http://www.miamidade.gov/ao.)
b. Department issued personal computers will be held for one week to ensure successful data transfer to the user's new PC.
c. ISTD staff will remove the hard drive from Department issued PCs and digital copiers. Hard drives will be destroyed prior to disposal.
d. Personal computers, digital copiers, monitors and printers will be transferred to the storage room; asset tags will be removed and sent to Finance with a list of the items being disposed of.
e. Items being disposed of will be sent to Internal Services with the list of items transferred. To document the transfer of custody, the signature of the Internal Services employee receiving the items will be obtained.
f. The Department's Commodities Management Division has vendors remove hard drives from leased copiers and fax machines. Hard drives will be destroyed prior to disposal.

13. Processing of Surplus Electronic Equipment Found in Terminal

a. Unclaimed computers, tablets and photographic equipment left unclaimed in Lost and Found will be inspected by ISTD staff for possible functional use by MDAD employees.
    i. Items deemed functional to staff will be transferred to ITSD, entered into the division's inventory system.
    ii. ISTD will inform the Finance and Strategy division of the transfer in order for the items to be recorded to the Fixed Asset Ledger and an inventory tag affixed to each item.
b. Division Directors or above, and other employees having a critical business need for computers, tablets, and photographic equipment must complete the Request for Surplus Electronic Equipment Form (available under the Forms section on the Intranet), see Exhibit G.
    i. The type of device and business purpose must be stated on the Request for Surplus Electronic Equipment Form.
    ii. The Request must be authorized by the employee's immediate supervisor, division director and assistant/deputy director.
    iii. All distributions will be made on a first come, first served basis.
    iv. ISTD will indicate on the Request the description of the device deployed, including model number, memory size (if applicable), and inventory tag number.
    v. The employee's signature on the Request at the time of transfer acknowledges responsibility to safeguard the County asset and return it upon separation, termination, or transference from MDAD.
    vi. Items not functional to MDAD can be made available to local law enforcement to enhance efforts directly safeguarding the Terminal and its users.

a) A Request For Surplus Electronic Equipment Form authorized by the Requestor's immediate supervisor and MDAD's Deputy Director must be submitted to ISTD.

VI. REVOCATION: None.

VII. CROSS REFERENCE:

A. Administrative Order No. 5-5, Acquisition, Assignment and Use of Telecommunication Devices and Network Resources.

B. Administrative Order No. 8-2, Use, Care, Control and Disposal of County Personal Property.

C. Implementing Order No. 6-8, Use of Cellular Telephones and Similar Wireless Devices While Operating County Vehicles.

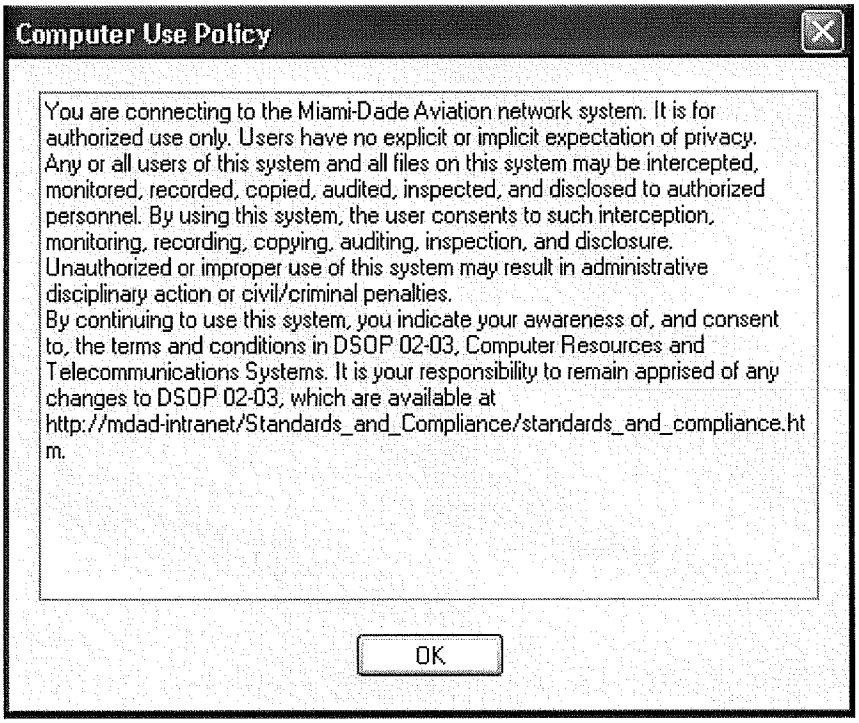
D. Departmental Standard Operating Procedure No. 06-01, Acquisition, Provision, and Use of Information Systems and Telecommunications Equipment and Services (Computing and Network Services).

E. Departmental Standard Operating Procedure No. 13-05, Procedures for Processing and Disposing of Lost and Found Items.

Emilio T. González, Aviation Director

Date: 4/21/14

Exhibit A


Computer Use Policy
You are connecting to the Miami-Dade Aviation network system. It is for authorized use only. Users have no explicit or implicit expectation of privacy. Any or all users of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized personnel. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure. Unauthorized or improper use of this system may result in administrative disciplinary action or civil/criminal penalties.
By continuing to use this system, you indicate your awareness of, and consent to, the terms and conditions in DSOP 02-03, Computer Resources and Telecommunications Systems. It is your responsibility to remain apprised of any changes to DSOP 02-03, which are available at http://mdad-intranet/Standards_and_Compliance/standards_and_compliance.htm.
OK

REQUEST FOR TELECOMMUNICATIONS SERVICE FORM

THIS AREA MUST BE COMPLETED

Date: _____ Date Service Requested: _____
Contact Person: _____ Priority 1- Emergency Work To Be Done Immediately
Contact Number: _____ Priority 2- Regular Scheduled Work
Division/Dept: _____

Requests for priority service must be submitted with written justification, and approved by the IST Manager Maurice Jenkins.

Location:

_____

Description Of Work Required: _____

_____

_____

Telephones: (Circle Choices)

Single line desk / Single line wall ☐
Meridian 3903 Display (4 Lines) ☐
Meridian 3904 Display (12 Lines) ☐

Phone Lines: (Circle Choices)

External Use Only ☐
Internal Use Only ☐
External & Internal Use ☐

Data Service: (Circle Choices)

Install Data Port ☐
Activate Data Port ☐
Delete Data Port ☐
Other:

FEATURES: (Circle Choices)

Bell chimes ☐
Call Forwarding ☐
Call Pick Up ☐
Call Transfer ☐
Speed Dial ☐
Caller Name Display: _____

Long Handset Cord ☐
Long Mounting Cord ☐
Fwd. If Busy to Ext. _____
Conference ☐
Headset ☐

Voice Mail w/Operator (Required) ☐
Long Distance Capability ☐
Fwd. If no answer to ext. _____
Intercom ☐
Other: _____ ☐ _____

Billable to:

(1) MDAD Telecomm _____ **(2) Project No:** _____ **(3) Other:** _____

Signatures Required For Processing:

Division Director's Approval: _____
(Print Name) _____
Division Director, IST (priority work only) _____

(FOR TELECOMMUNICATIONS USE ONLY)

Date Received _____ *Due Date* _____
IFON Number _____ *ORG Code* _____
SR Number _____

(1) Per Contract _____ *(2) Price Quote* _____ *(3) Work to be done on T&M* _____

Fax to Telecommunications for Processing: Lorraine Jones 305-876-0932 Chelsy Copin 305-876-7131 Barbara Grant 305-876-8078
Fax Number 305-876-0933 revised 3/10

Exhibit C

Information Systems - Network Account Request Form

(This form must be completed by the person who will be using the account)

Employee Status: ☐New Hire - Start Date: _____ ☐Permanent ☐Intern ☐Temporary

Account Duration - (non-permanent employee): Start Date: _____ End Date: _____

Please select type of account required:

☐ **Network/Email Account**

Last Name: _____

First Name: _____

Middle Name: _____

Job Title: _____

Division/Section: _____

County Employee ID Number: E-_____

Location: _____

Telephone (include pre-fix): _____

Fax (include pre-fix): _____

☐ **Central Registration System (CRS) Account (Needed for ERP Systems Access)**

Select one or both: ☐ ERP Financials ☐ ERP HR (Time & Labor)

User ID: _____ **(ISD Use only)**

Social Security Number: _____ **(Last 4 digits only)**

Department No: _____ Division No: _____ Location No: _____

Verification Code: _____ **(maximum 10 characters)**

Immediate Supervisor Information

Last Name: _____ First Name: _____ (please print)

Title: _____ (please print)

Approvals:

Immediate Supervisor:

Signature: _____ Date: _____

Division Director:

Please Print: _____

Signature: _____ Date: _____

Please allow 24 hours for processing. Incomplete Forms will cause a delay in processing.
Submit Request Form to Fax Number: 305-869-4164.

Exhibit D

INFORMATION SYSTEMS DIVISION
REQUEST FOR SERVICE FORM

Full Name: _____ Title: _____

Location: _____ Division/Section: _____
(Bldg, Floor, Room #)

Telephone: _____ Fax: _____ Contact Person: _____

Employee Status: ☐New Hire - Official Start Date: _____ ☐Intern ☐Temporary ☐ Permanent

Please Indicate Type of Service Required

☐ New Workstation (includes PC, Monitor, Printer, Microsoft Office Suite, Microsoft Outlook)*

☐Upgrade of existing workstation ** ☐Relocate existing workstation

Scheduled date of relocation: _____

☐Network Applications: _____
(i.e. PGTS, Supply, Work Order System, Security Badge, ERP Financials, ERP HR, etc.)

☐Other (specialized) PC Software: _____
(i.e. Adobe Acrobat, Microsoft Visio, Microsoft Project, etc)

☐Other Hardware:* _____
(i.e. Color printer, laptop, scanner, plotter)

PLEASE JUSTIFY REQUEST: ** _____

_____

_____

_____

_____

_____

APPROVALS:

Immediate Supervisor: _____ Title: _____
(Print Name)

_____ Date: _____
(Signature)

Division Director: _____ Division: _____
(Print Name)

_____ Date: _____
(Signature)

***** Assistant Director:** _____ Title: _____
(Signature)

*** Only required for new workstations and upgrade of existing workstation

* *Please allow a minimum of 2 weeks for processing request. Request Fax Number: (305)-869-4164*
** *Request will not be processed without proper justification.*

Exhibit E

MIAMI-DADE AVIATION DEPARTMENT (MDAD)
TERMS AND CONDITIONS FOR MOBILE DEVICES

This document contains MDAD's Terms and Conditions for the use of Personal and County-issued devices, such as iPhones, IPADs, Microsoft Windows Mobile Devices, Android Devices, etc. on the MDAD Microsoft Exchange messaging network.

Carefully read Section V-10, Department Network Access from Mobile Devices, in the Departmental Standard Operating Procedure No. 02-03, Computer Resources and Telecommunication Systems. When you have completed reading the terms and conditions, and fully understand the information contained, click on the "I Agree" checkbox and submit your agreement to Information Systems and Telecommunications.

Only individuals who have agreed will have access to MDAD email services on their mobile device. By clicking on the "I Agree" checkbox, you agree to all terms and conditions for enrollment to access MDAD Enterprise Network Service.

As a reminder, Miami-Dade County is a public entity subject to Florida's public records laws, including Florida Statutes, Chapter 119. Information stored on the device, including, but not limited to, email messages, text messages, contacts, appointments, photographic images, downloads and websites accessed, are subject to public records disclosure, and with limited exceptions, are not exempt from such disclosure.

If you no longer wish to use these services, contact the Help Desk at X5900. Please be aware that removing yourself from this service WILL require a system wipe. A system wipe may cause the device to be restored factory settings.

☐ I Agree

☐ I Do Not Agree

MDAD User ID _____

Full Name _____

Division _____

Exhibit G

INFORMATION SYSTEMS DIVISION

REQUEST FOR SURPLUS ELECTRONIC EQUIPMENT

Full Name: _____ Title: _____

Division: _____ Telephone: _____

Type of Device Requesting: _____

Please Provide Business Purpose for Device Requested: _____

_____

APPROVALS:

Immediate Supervisor*: _____ Title: _____
(Print Name)

_____ Date: _____
(Signature)

Division Director: _____ Title: _____
(Print Name)

_____ Date: _____
(Signature)

Assistant/Deputy Director*: _____ Date: _____
(Signature)

*Requests by outside law enforcement agencies must include authorization by immediate supervisor and MDAD Deputy Director.

To Be Completed by Information Systems:

Description of Device Deployed: _____

Model Number/Memory Size: _____ County Asset Tag No. _____

To Be Completed When Employee Takes Possession of Device:

Employee's signature indicates he/she has possession of device noted; will safeguard this County asset; and surrender it upon separation, termination or transference from MDAD.

Employee's Signature: _____ Date of Transfer: _____