



ACCESS POINT KEY ISSUE FORM

KEY (S) #
CHARGER (S) #

CYBERVAULT CYBERSHARED CYBERKEY SECURITY KEY/CODE

ACCESS POINT KEY HOLDER - RESPONSIBILITIES, POLICIES & PROCEDURES AGREEMENT

As a Memphis-Shelby County Airport Authority (MSCAA) authorized Access Point Key Holder, I understand, will adhere to and will be held accountable to the following Access Point Key Holder Policies & Procedures:

1. **CyberKeys:**



CYBERVAULT



CYBERKEY



CYBERLOCKS



UPDATER



CHARGERS

- a. **Expiration:** All CyberKeys will expire **8** hours after each updating/checkout.
 - b. **Charging & Updating:** (CyberKeys are rechargeable and must be charged to work/update)
 - 1) **CyberVault Keys:** Automatically charged & updated via the CyberVault.
 - 2) **CyberShared Keys:** Manually charged & updated via the issued Chargers and by placing in a CyberKey Updater.
 - a) You must enter your pin number followed by the “#” button in order to update your key using the “Updater”. **Check** your key in the Updater “**Test Lock**” before you leave.
 - c. **Malfunctioning/Damaged CyberKeys:** Coordinate with CyberSystem Administrator via email (AirportSecurityCoordinator@flymemphis.com) for repair/replacement as needed.
 - d. **CyberVault Checkout:** You must swipe your **VALID** MEM Issued SIDA ID Badge and enter your pin number followed by the “#” button in order to Program and Checkout a CyberKey from a CyberVault. **Check** your key in the Vault “**Test Lock**” before you leave. Keys **will ALARM** if not returned to the CyberVault within 8 hours.
 - e. **CyberShared Checkout:** It is the Company Certifying Officials’ responsibility to keep unissued CyberShared Keys **secured** at all times and maintain detailed logs of who can access the secured CyberShared Keys and all issuances of CyberShared Keys.
2. As an MSCAA Access Point Key Holder of my Company, I understand that I will be held accountable for any Access Point Key issued to me by the MSCAA. I further understand that at any time the MSCAA and/or the Transportation Security Administration Inspectors (TSI) can perform an accountability audit of my Access Point Key(s).
 3. At **no time** can an Access Point Key Holder allow another person to possess/use their Access Point Key. Treat your Access Point Key as you would your Airport issued SIDA/AOA ID Badge. The same rules, violations and penalties apply to their misuse.
 4. I understand that I **must** surrender my Access Point Key at any time upon demand of my Company Certifying Official, Airport Police Officer, Airport Operations Duty Manager, Airport Security Coordinator (ASC) or Alternate (AASC), and/or CyberSystem Administrator.
 5. I understand that it is my responsibility to report **immediately** any Access Point Key Lost or Stolen to the MSCAA Airport Police Department, via filing a Police Report (Tel: 901-922-8298); **and** the ASC, via email (AirportSecurityCoordinator@flymemphis.com).
 6. The MSCAA reserves the right to charge the Tenant Company and/or Employee for all costs associated with a lost/stolen/damaged Access Point Key. The costs may include the purchasing/rekeying/recoding/repairing of the lock(s), purchasing/programming/repairing the new Access Point Key, and all labor associated with this process.
 7. I will **IMMEDIATELY** return my issued Access Point Key, when I no longer have a “**VALID**” SIDA / AOA ID Badge or a Job Related need, to my Company Certifying Official or MSCAA CyberSystem Administrator.
 8. Violations of the Access Point Key Policies and Procedures **will** subject the Access Point Key Holder and/or Airline/Tenant Company to be fined by the MSCAA and/or TSA and cause your Access Point Key Holder status to be **Permanently Revoked**.

KEY HOLDER - INFORMATION:	SIDA/AOA ID BADGE #	COMPANY	DEPARTMENT	CYBERKEY ACCESS GROUP
----------------------------------	---------------------	---------	------------	-----------------------

I CERTIFY THAT I HAVE A **VALID SIDA / AOA** ID BADGE AND HAVE A **JOB RELATED** NEED TO BE ISSUED A MSCAA ACCESS POINT KEY. BY SIGNING THIS FORM, I CERTIFY THAT I HAVE RECEIVED THE ABOVE LISTED CYBERVAULT ACCESS OR ACCESS POINT KEY AND THAT I UNDERSTAND MY RESPONSIBILITIES AS AN ACCESS POINT KEY HOLDER AND THAT I WILL ADHERE TO AND BE HELD ACCOUNTABLE TO THE POLICIES AND PROCEDURES OUTLINED IN THIS FORM BY MSCAA.

(LAST NAME)	(FIRST NAME)	(SIGNATURE)	(DATE)
(CELL PHONE TEL #)	(WORK PHONE TEL #)	(EMAIL ADDRESS)	

KEY HOLDER COMPANY CERTIFYING OFFICIAL - APPROVAL

I CERTIFY THAT THE ABOVE EMPLOYEE/CONTRACTOR HAS A **VALID SIDA / AOA** ID BADGE AND HAS A **JOB RELATED** NEED TO BE ISSUED AN ACCESS POINT KEY.

(CERTIFYING OFFICIAL - FULL NAME)	(CERTIFYING OFFICIAL - SIGNATURE)	(CERTIFYING OFFICIAL - DATE)
-----------------------------------	-----------------------------------	------------------------------

MSCAA ASC/AASC OR CYBERKEY ADMINISTRATOR USE ONLY!

- PERMANENTLY REVOKED
- TERMINATED
- OTHER:

(ISSUED - DATE)	(ISSUED BY - NAME)	(ISSUED BY - SIGNATURE)	(APPROVED BY - SIGNATURE)	(STATUS CHANGE)	(RECEIVED BY)	(DATE)
-----------------	--------------------	-------------------------	---------------------------	-----------------	---------------	--------