

MAIL SIGNED ORIGINAL TO:  
 DGS/Office of Human Resources  
 P.O. Box 989052, MS 402  
 West Sacramento, CA 95798-9052  
 Attn: OHR ABMS Security Administrator

**\*\*\* Please submit the original signed OHR-2 to the address above to prevent delays in processing.**  
**\*\*\* DO NOT fax or submit copies. DO NOT submit to the ABMS team.**

**1. EMPLOYEE INFORMATION**

NAME		ABMS NUMBER (Required)
DIVISION/OFFICE	BPM REGION (If applicable)	WORK PHONE
POSITION NUMBER	CLASSIFICATION	WORK LOCATION
REASON FOR ACCESS (Adding / Changing access only)		NAME OF PERSON BEING REPLACED (If applicable)

**2a. ABMS ACCESS**

**2b. PAL ACCESS**

ACTION	TYPE OF ACCESS (Check <u>One</u> )	ACTION	TYPE OF ACCESS (Check <u>One</u> )
ADD CHANGE REMOVE	PERSONNEL LIAISON ATTENDANCE CLERK TRAINING COORD OTHER:	ADD CHANGE REMOVE	PERSONNEL LIAISON ATTENDANCE CLERK TIMEKEEPER OTHER:
ABMS ACCESS TO EMPLOYEES IN (Complete <u>One</u> )		PAL ACCESS TO EMPLOYEES IN (Complete <u>One</u> )	
OFFICE NAME:		OFFICE NAME:	
BPM REGION:		BPM REGION:	
AGY/UNIT(S):		AGY/UNIT(S):	
<b>ABMS SUPERVISOR ACCESS</b>		<b>PAL SUPERVISOR ACCESS</b>	
ABMS supervisor access is automatic. Login with your PAL username and the initial password of the last 4-digits of your SSN plus a zero.		<ul style="list-style-type: none"> <li>• PAL APPROVAL: This form <u>is not</u> required to approve PAL.</li> <li>• <input type="checkbox"/> I need access to <u>post</u> time for my employees.</li> </ul>	

SUPERVISORS: If you cannot access your employees in ABMS or PAL, have your Attendance Clerk update the supervisor field on your staff's ABMS records.

**3. EMPLOYEE STATEMENT OF UNDERSTANDING**

I hereby acknowledge receipt and have read and understand the provisions and restrictions contained in the DGS-ABMS Security Guidelines provided with this document. (Employee should retain for his/her records.)

I fully understand that any violations of security policies and procedures are subject to disciplinary action. Immediate corrective action may result in revocation of access to the Confidential Human Resources Personnel data of the Department of General Services (DGS-ABMS). Any violation of the California Information Practices Act (1977) may also result in criminal and/or civil action.

I also understand that unauthorized access, attempting access or use of any computer systems and/or data of the State of California is a violation of Section 52 of the California Penal Code, and is subject to prosecution.

EMPLOYEE SIGNATURE 	DATE
----------------------------------------------------------------------------------------------------------	------

**4. AUTHORIZED SIGNATURE**

I attest this is an employee of DGS who requires access to ABMS and/or PAL for their assigned duties to this Office/Branch. She/he must have access to confidential HR Personnel data in order to perform legal, statutory and/or government duties.

OFFICE/BRANCH CHIEF SIGNATURE 	DATE
CONTACT PERSON FOR THIS HR-1 REQUEST	WORK PHONE

**Do not submit Security Guidelines on pages 2 – 5 with original signed OHR-2 form.**

**DEPARTMENT OF GENERAL SERVICES**

**OFFICES OF HUMAN RESOURCES**

**ACTIVITY BASED MANAGEMENT SYSTEM  
(ABMS)**

**SECURITY  
GUIDELINES**

Prepared by:

Office of Human Resources  
Activity Based Management System

Revised September 2004

**THIS PACKAGE SHOULD BE REPRODUCED AND DISTRIBUTED AS NEEDED  
AND RETAINED BY THE REQUESTOR OF ABMS HR ACCESS. DO NOT  
SUBMIT THE SECURITY GUIDELINES WITH THE OHR-2 REQUEST.**

## SECURITY/CONFIDENTIALITY

The purpose of these guidelines is to define the Department of General Services-Activity Based Management System (DGS-ABMS) security requirements to all users of the confidential Human Resources (HR) portion of the DGS-ABMS computer database. These are intended as guidelines only and any questions or need for more information should be directed to your Local Area Network (LAN) Administrator.

The DGS-ABMS maintains a dedicated computer program that houses numerous systems of records, which contain confidential and sensitive data. Although automation provides valuable information, access to centrally stored machine-readable data increases the risk of unwarranted disclosure of this data. Therefore, DGS-ABMS restricts such access to those individuals who have a bonafide business need and legal justification for such access. Access is authorized by individual position responsibilities (i.e. Personnel liaisons access is different than Attendance Clerks access).

DGS-ABMS maintains several automated security control systems, which will continue to be modified as needed, or when more sophisticated technology becomes available. However, individuals using or having control over confidential HR data must understand DGS-ABMS requirements for handling such information.

Careless, accidental or intentional disclosure of information to unauthorized persons can have far-reaching effects, which may result in civil or criminal actions against those involved in the unauthorized disclosure (please refer to California Penal Code Section 502 and the California Information Practices Act [1977]). To reduce the risk, it is necessary for DGS-ABMS to establish and enforce these requirements for all system users. Please read this document and the attached Statement of Understanding form, carefully to ensure understanding before signing the form.

## CONTROLLING ACCESS TO EQUIPMENT

1. Access is granted to an individual based on four factors:
  - a. They must have access to confidential HR Personnel/Payroll data in order to perform their legal, statutory or government duties. (If applicable, a "Justification Statement" must accompany this document if the individual does not have a classification that denotes their employment is within the Personnel/Payroll area.);
  - b. Must be a bonafide employee of the DGS and specifically of the requesting office;
  - c. Completion of the Security Authorization form, signed by the ABMS Security Administrator, and Office Chief attesting to the above mentioned factors; AND
  - d. Completion of the "Statement of Understanding," acknowledging that the individual has read and understands these guidelines.
2. These factors are reviewed and the ABMS Security Administrator who represents the Chief, Office of Human Resources grants access.
3. Once access has been approved, the individual is assigned a "User ID." The initial password will be the last four digits of the individual's Social Security Number followed by a Zero. Upon initial entry, the individual will be required to use this number to gain access and to select a new password known only to the user. This unique password is the essential security system element that protects both the individual and DGS-ABMS confidential HR data from unauthorized disclosure.
4. **PASSWORDS:** *the individual owner must protect their password at all times. It is never to be disclosed or "shared" with anyone.* The failure to protect a password may result in a 30-day suspension from access to the DGS-ABMS database. Any future failure to protect the password may result in permanent removal of access. (It should be noted that these actions are not to be misconstrued as punitive - merely a corrective action and a safety precaution to limit further possible harm to the security of DGS-ABMS confidential HR data.) Disciplinary or punitive action is determined on a case-by-case basis and may be in addition to other legal actions resulting from violating state law.
5. **CAUTION:** an individual may be considered to have "shared" their password if another individual uses an "active" terminal/PC under the following conditions:
  - a. An individual, having logged-on, leaves the active terminal/PC for an undetermined timeframe (i.e., breaks, lunch, meeting) and another individual enters data or a transaction on the active terminal/PC.
  - b. Either for "training" purposes or for someone who is waiting for access approval; an individual "logs-on" to allow the other person to key-enter data/transactions.

Once an individual logs-on the system, any and all transactions or data keyed-in under that individual's UserID/password, belongs to that individual - regardless of the circumstances or the legality of the information entered. The liability; however, for any illegal transactions belongs to the owner of the password - not the person who entered the transaction. Therefore, each individual must log-off (deactivate a session) prior to leaving a terminal/PC.

Such liability may result in civil and/or criminal actions and be punishable under Section 502 of the California Penal Code.

### **RESPONSIBILITY FOR PROTECTING CONFIDENTIAL DATA**

The responsibility for protecting confidential and sensitive data residing on the DGS-ABMS computer system is a shared effort. DGS-ABMS has an overall role in overseeing the total security effort. DGS-ABMS's responsibility encompasses the area of data, and access security. The area of access security at the initial point resides with department management selecting and requesting access for an individual that meets the criteria, previously mentioned. DGS-ABMS will then verify, and if necessary, require justification for an individual that does not appear to meet the criteria. This area, including protection of access (passwords), is fairly straightforward and easily understood.

The area that is not so easily understood is the level of protection of confidential data that is either viewable on individual video monitors or extracted from a printer from the DGS-ABMS system. This data once it is removed or viewable within the offices comes under the protection and responsibility of the staff and management of that office. It therefore behooves staff and management to know and understand the restriction on disclosure of confidential information delineated in the California Information Practices Act (1977). Precautions to ensure that all-necessary physical security interventions have been implemented are imperative to avoid inadvertent access or disclosure to unauthorized individuals. Any failure in this area could result in violations in which individuals, staff and/or management may be held liable. The DGS-ABMS has no responsibility or control over the physical security area of the individual offices.

Each individual must be aware of the potential disclosure of confidential HR data either through unlawful use of a password, unattended active terminal/PC, leaving confidential information unattended at the printer, or through inadvertent disclosure. The later problem is usually the result of unauthorized individuals viewing confidential data via a screen or document left out on a desk or at a printer. Regardless of the manner of exposure, the individual controlling the documents and/or the physical security of the office is responsible for the violation and any subsequent legal consequences as a result of the disclosure. Therefore, all hard copies (including printouts) of data extracted from the DGS-ABMS computer system remain confidential, but are to be protected by Office personnel from unauthorized disclosure as stipulated in the California Information Practices Act (1977).

The Department of General Services adheres to the regulations and requirements set forth in the California Information Practices Act (1977) as well as the Federal Privacy Act (1974). Each office staff member accessing confidential HR personnel data is encouraged to read and follow the tenets of both these State and Federal statutes.

### **GUIDELINES TO THE INFORMATION PRACTICES ACT OF 1977 RULES OF CONDUCT FOR EMPLOYEES**

Employees responsible for the collection, maintenance, use and dissemination of information about individuals which relates to their personal life, including their employment and medical history, financial transactions, marital status and dependents, for example, shall comply with the provisions of the Information Practices Act, Civil Code Sections 1798 through 1798.78. The guidelines to the Act issued by the Office of Information Practices shall be used as a basic source of guidance in administering the Act's provisions.

Employees shall not require individuals to disclose personal information which is not necessary and relevant to the lawful State function for which the employee is responsible.

Employees shall make every reasonable effort to see that inquiries and requests by individuals for their personal records are responded to quickly and without requiring the individual to unnecessarily repeat his or her inquiry to others.

Employees shall assist individuals who seek information pertaining to themselves in making their inquiry sufficiently specific and descriptive so as to facilitate locating the records requested.

Employees shall respond to inquiries from individuals, and requests from them to review, obtain copies of, amend, correct or dispute their personal records in a courteous and businesslike manner, and in accordance with Sections 1798.30 through 1798.42 of the Civil Code.

Employees shall not disclose personal information relating to individuals to unauthorized persons or entities. The improper disclosure of personal information may be cause for disciplinary action.

Employees shall not seek out or use personal information relating to others for their own interest or advantage. The intentional violation of this policy may be cause for disciplinary action.

Employees responsible for maintenance of records containing personal information shall take all necessary precautions to assure that proper administrative, technical and physical safeguards are established and followed in order to protect the confidentiality of records containing personal information, and to assure that such records are not disclosed to unauthorized individuals or entities.