SAUDI ARABIAN OIL COMPANY (Saudi Aramco) **GENERAL INSTRUCTION MANUAL**		G. I. Number Approved 299.120	
ISSUING ORG.	IT/INFORMATION PROTECTION & TECHNOLOGY PLANNING DEPARTMENT / INFORMATION PROTECTION MANAGEMENT DIVISION	ISSUE DATE 03/01/2010	REPLACES December 2005
SUBJECT	Sanitization and Disposal of Saudi Aramco Electronic Storage Devices and Obsolete/Unneeded Software	HKA	PAGE NO. 1 OF 12

Content

This General Instruction (GI) document outlines the methods and procedures for the sanitization of electronic storage devices being transferred, repaired, surplussed or decommissioned. The text of this Instruction covers:

1 Purpose

This General Instruction defines company-wide standards for the proper sanitization of any electronic storage device being disposed of, returned to manufacturer, donated or surplussed to ensure that Saudi Aramco sensitive information do not get disclosed to unauthorized users. It also outlines the procedures for the disposal of obsolete computer software.

All data must be removed from electronic storage devices whenever they are disposed of, transferred, surplussed or decommissioned. It must be done in such a way that data cannot be recovered. The process of simply erasing data or reformatting the electronic storage devices are not acceptable because it does not prevent data from being recovered by technical means.

2 Scope

This General Instruction covers all fixed and removable electronic storage devices owned, leased, operated and maintained by Saudi Aramco. This includes, but is not limited to hard drives and other removable drive disks, diskettes, tapes, optical disks, non-volatile memory devices (such as memory sticks and cards or USB memory storage), and PDA’s.

Any electronic storage devices currently available, or that become available in the future due to new technology, are also covered by this Instruction.

3 Definitions

The following terms will be used in this document:

AM&RD: Al-Midra and Reclamation Division.

AREA IT: Area Information Technology Department

* **CAWIMU**: Central Area Workstation Installation & Maintenance Unit.

CD: Compact Disc.

Coercivity: Magnetic media is divided into three types (I, II, III) based on their coercivity. Coercivity of magnetic media defines the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. The level of magnetic media coercivity must be ascertained before executing any degaussing procedure.

Computer Software: Refers to the original computer software media that includes – but not limited to diskettes, CDs and documentation acquired by the Company as well as any copies.

CSA: Computer Security Administration.

CSL: Computer Security Liaison

Degauss: Process that reduces the magnetic flux on media virtually to zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is more effective than overwriting magnetic media.

Degausser: Device used to remove data permanently from magnetic storage medium. The end result is the total incapacitation of the storage device so that it may never work again.

Electronic Storage Device: is any technology used to place, keep, and retrieve data on a long-term basis. This includes, but is not limited to: magnetic media (including hard drives, magnetic tape, floppy, and other removable drive disks), optical disks, non-volatile memory devices (including memory sticks and cards or USB memory storage), and PDAs.

* **IPMD**: Information Protection Management Division.

* **C&CWU**: Computer & Communication Warehouse Unit.

Obsolete Hardware: Any Computer based device that was used within Saudi Aramco and is no more required for use. (Saudi Aramco has specific guidelines regarding obsolescence of equipment and this term incorporates that all processes were followed to declare hardware obsolete)

Obsolete Software: The software is no longer produced at the version or release level indicated on the original software diskettes and in the documentation.

Sanitizing: The process of removing the data on the media before the media is reused in an environment that does not provide an acceptable level of protection for the data.

Software Erasure Report: The output of the sanitization software certifying that the electronic media was sanitized.

** **Degaussing Form**: A form to certify the degaussing of an electronic storage device as per the Computer & Communication Warehouse Unit operational procedures.

SCO: Supporting Computer Organization (The support organization responsible for the computer center).

* **Unneeded**: The original software diskettes, CDs, and documentation have been turned in by the user to the C&CWU and C&CWU has decided that the software is surplus to Company needs.

4 General Information

4.1 Data must be reviewed and backed up, as deemed necessary, before any electronic storage device is sanitized or destroyed.

4.2 Before any electronic storage device is loaned, transferred, decommissioned, donated, surplussed or being disposed of all data must be completely erased and made unreadable (sanitized) using the standards specified in this document, unless there is specific intent to transfer the particular software or data within the company. This means that no storage device or storage component may be handed over until all data, on any device being removed, has been sanitized or destroyed.

4.3 The transportation of electronic storage devices to a different location, for sanitization or destruction, need to be adequately secured to prevent possible data theft during transportation.

4.4 Whenever licensed software is resident on any electronic storage device being transferred, or otherwise disposed of, the terms of the license agreement must be followed.

4.5 After the sanitization of hard drives or other electronic storage devices are completed, the process must be verified and certified by the CSL or his/her authorized representative and records maintained as specified in this document.

5 Sanitization Specifications

The sanitization of electronic storage devices need to be done in such a way that all data are completely erased and made unreadable. The following methods must be utilized to ensure the proper sanitization of electronic storage devices.

- Overwriting
- Degaussing
- Physical Destruction

5.1 Software Specifications for Overwriting

Overwriting is process of replacing the data previously stored on electronic storage device with a predetermined set of meaningless data so that the old data cannot be recovered.

All software products and applications used for the overwriting process must meet the following specifications:

5.1.1 The data must be properly overwritten by overwriting all locations three (3) times: (1) the first time with a random character, (2) the second time with a specified character, (3) the third time with the complement of that specified character.

5.1.2 Sanitization must not be considered complete until three overwrite passes and a verification pass is completed.

5.1.3 The software must have the capability to overwrite the entire electronic storage device, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data.

5.1.4 The software must have the capability to overwrite the data using a minimum of three cycles of data patterns on all sectors, blocks, tracks, and any unused disk space on the entire device medium.

5.1.5 The software should have the capability to read and write to any hardware disk configuration (e.g. RAID) so that data written across multiple storage devices can be permanently deleted.

5.1.6 The software must have a method to verify that all data has been removed.

5.1.7 Sectors not overwritten should be identified.

5.2 Degaussing Specifications

Degaussing reduces the magnetic flux on media virtually to zero by applying a reverse magnetizing field and renders any previously stored data on magnetic media unreadable. Electronic storage devices cannot be re-used after degaussing. Degaussing is utilized if a device is faulty and cannot be sanitized by normal means (software).

Degaussing machines **must** meet the following criteria:

5.2.1 The degausser must be able to erase working and non-working electronic storage devices;

5.2.2 High energy “able to degauss large volume”;

5.2.3 The degausser must render the electronic storage devices from being used again;

5.2.4 Able to handle almost all magnetic device formats e.g. diskettes, hard disk, LTD, and memory;

The following recommended procedures should be followed when electronics storage devices are degaussed:

5.2.5 Follow the product manufacturer’s directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing.

5.2.6 Shielding materials (cabinets, mounting brackets), which may interfere with the degausser’s magnetic field, should be removed from the electronic storage devices before degaussing.

5.2.7 Electronic storage device platters should be in a horizontal direction during the degaussing process.

5.3 Physical Destruction

Electronic storage devices should be physically destroyed when they are being disposed of or cannot be repaired or sanitized for reuse. Physical destruction should be accomplished to an extent that precludes any possible further use of the devices.

This can be attained by:

5.3.1 Physical force such as pounding with a sledge hammer or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the electronic storage device so it cannot be reinserted into a functioning computer.

5.3.2 Any other means that will destroy the body and contents of the electronic storage device.

5.3.3 Electronic storage devices such as tapes, floppies, removable flash cards, ZIP disks etc., must be sanitized, if possible, prior to destruction e.g. demagnetize tapes.

5.3.4 Electronic storage devices must be physically destroyed in such a way that the recovery of the media is improbable e.g. shredding of CDs.

6 Sanitization Process of Hard Drive and Surplus Computers

6.1 Workstations & Laptops

6.1.1 Before any computer, laptop or hard drive is loaned, donated, transferred, surplussed, being disposed of or transferred to Information Technology Warehouse; it must be sanitized (overwriting) in accordance with the standards specified in this document, with the process verified and certified by the CSL or his/her authorized representative, unless there is specific intent to transfer the particular software or data within the company.

6.1.2 Before submitting an asset request for the removal of a workstation, all hard drives must be sanitized (overwriting), unless there is specific intent to transfer the particular software or data within the company.

6.1.3 After sanitization the software erasure report must be signed by the CSL or his/her authorized representative to validate and certify that the computer was sanitized. The CSL will keep a copy of the software erasure report and attach the original software erasure report to the computer or hard drive.

* If the hard drive cannot be sanitized it must be forwarded to C&CWU or Area IT, as applicable, for degaussing. The CSL or his/her authorized representative must approve and sign the degaussing form prior to sending the hard drive to be degaussed. The CSL will keep a copy of the degaussing form and attach the original to the computer or hard drive.

* 6.1.4 Computers/hard drives to be destroyed or surplussed must be sanitized and transferred to the C&CWU warehouse in Dhahran or respective responsible unit for Saudi Aramco International offices, per the return procedures specified in the IT Asset management System.

* 6.1.5 Hard drives, collected for repair or return to a vendor/manufacturer need to be sanitized (overwriting), with the process verified and certified by the CSL or his/her authorized representative, prior to collection. If the hard drive cannot be sanitized (overwriting), it needs to be degaussed by C&CWU or Area IT, as applicable, prior to the collection by the vendor/manufacturer. If an electronic storage device need to be sent outside Saudi Aramco for repair or data recovery the following steps must be followed if the hard drive cannot be sanitized.

- * The proponent or owner of the data (as per GI-710.002), resident on the storage device, needs to approve the transfer of the storage device outside the company.
- A non-disclosure agreement must exist between the vendor and Saudi Aramco.

6.2 Servers

* 6.2.1 Before any server is loaned, donated, transferred, surplussed, being disposed of, or transferred to Information Technology Warehouse; it must be sanitized (overwriting) by the SCO in according with the standards specified in this document, unless there is specific intent to transfer the particular software or data within the company.

* 6.2.2 Before submitting an asset removal request of a server, all hard drives must be sanitized (overwriting), unless there is specific intent to transfer the particular software or data within the company.

* 6.2.3 After sanitization the software erasure report must be signed by the SCO to certify that the server was sanitized. The SCO will keep a copy of the software erasure report and attach the original software erasure report to the Server or hard drive.

If the hard drive cannot be sanitized (overwriting) it must be degaussed by SCO or forwarded to C&CWU or Area IT for degaussing. If the hard drive will be sent to C&CWU or Area IT, SCO must approve and sign the degaussing form prior to sending the hard drive to be degaussed. SCO will keep a copy of the degaussing form and attache the original to the computer or hard drive.

* 6.2.4 Computers/hard drives to be decommissioned, destroyed or surplussed must be sanitized and transferred to the supporting computing organization, per the return procedures specified in the IT Asset management System.

* 6.2.5 Hard drives, collected for repair or return to a vendor/manufacturer need to be sanitized (overwriting) by the SCO prior to the collection. If the hard drive cannot be sanitized (overwriting), it needs to be degaussed by the SCO or forwarded to C&CWU or Area IT for degaussing prior to the collection by the vendor/manufacturer.

7 Physical Destruction of Electronic Storage Devices

7.1 Before any electronic storage device is disposed of, the user must either sanitize or physically destroy the electronic storage device, e.g. shredding of a CD.

* 7.2 Bulk Electronic storage devices to be destroyed or disposed of can be transferred to the C&CWU warehouse in Dhahran, per the return procedures specified in the IT Asset management System. Saudi Aramco International offices transfer their Bulk Electronic storage devices to their respective unit for destruction.

7.3 Before submitting an asset request for the removal of the Bulk Electronic storage devices the storage devices must be sanitized if possible.

* 7.4 C&CWU will collect the bulk electronic storage devices and store it in a secure area until enough quantities have been collected for destruction. C&CWU will then complete reclamation form (SA-112) and the Digital Records Destruction Request Form to initiate the destruction.

* 7.5 SCO can also destroy bulk electronic devices, for their respective data centers, by completing reclamation form (SA-112) with Division Head signature and the Digital Records Destruction Request Form. The SCO will collect and erase/degauss the bulk electronic storage devices prior to destruction.

* 7.6 The physical destruction of the media has to be witnessed by proponent representative, Information Protection Management Division (IPMD) representative, Computer Security Administration (CSA) representative, Reclamation representative, other organizations representatives as deemed necessary.

* 7.7 IPMD representative must complete section E of the Digital Records Destruction Request form summarizing the result of the destruction operation.

7.8 All representatives must signoff on section F of the Digital Records Destruction Request form and the Reclamation Form (SA-112);

7.9 Distribute copies of the completed forms to all representatives.

8 Unneeded and Obsolete Software

* 8.1 Unneeded and obsolete computer software and accompanying documentation from all Company sites, will be transferred to C&CWU, by submitting an eService request and per the software return procedures specified in the IT Asset management System.

8.2 Any "installed" versions of unneeded and obsolete software resident on computer hard disks must be deleted. If the software manufacturer has authorized user-produced backup diskettes or CDs of the software and/or user-reproduced copies of the original software documentation, such diskettes or CDs must be destroyed by the user organization.

* 8.3 C&CWU will collect unneeded and obsolete computer software and accompanying documentation and submit them to the Al-Midra and Reclamation Division (AM&RD) using Form 112, available form Material Supply, to initiate the transfer. The form will be accompanied by a memorandum to AM&RD requesting that a mutual time be arranged for a representative from each organization (C&CWU and AM&RD) to witness the destruction of the unneeded or obsolete software. The memorandum must be signed at the Division Head level.

* 8.4 The C&CWU will arrange a mutual time for a representative from concerned organizations to witness the destruction of the unneeded and obsolete workstation software.

* 8.5 Electronic storage devices and software disposal will be completed in the presence of C&CWU and the AM&RD representatives at the agreed-upon time.

8.6 AL-MIDRA AND RECLAMATION DIVISION (AM&RD)

* 8.6.1 After arrangements have been made for a destruction date and an AM&RD witness has been designated for the destruction, assign the Form 112 a control number and give the C&CWU representative a copy for their records.

* 8.6.2 The C&CWU representative meets the AM&RD representative at the disposal site. Both representatives bring their copies of the Form 112 for the software to be destroyed.

8.6.3 The representatives witness the disposal of the software and documentation.

NOTE
The MEPA (Meteorology and Environmental Protection Administration) recommends the burial of materials, NOT BURNING THEM

8.6.4 Both Representatives date and sign in the appropriate areas of both Forms.

9 Roles & Responsibilities

* 9.1 Computer Operation Department \ Windows Infrastructure Division

- Maintain and provide the sanitized software to authorized users.

9.2 Computer Security Liaison

- * Verify and certify the sanitization process, as outlined in this document, by signing the software erasure report or the degaussing form for electronic storage device being disposed of, returned to manufacturer, donated or surplussed. If the CSL is not available e.g. remote area the CSL or department manager can authorize an individual to sign on his/her behalf.
- * File one copy of the software erasure report or the degaussing form; and attach the original to the sanitized storage device.
- * Provide the necessary support to ensure that the software erasure reports for equipment under his control is signed on request.

9.3 Computer Security Administration

- Maintain awareness to the CSLs to their responsibilities regarding the sanitization of electronic storage devices.

* 9.4 Information Protection Management Division

- Maintain this General Instruction document
- ** Witness the physical destruction events

* 9.5 Area IT Department / Central Area Installation & Maintenance Division / Central Area Workstation Installation & Maintenance Unit

- Maintain the capacity and hardware to degauss electronic storage devices. Perform degaussing of electronic storage devices received and attach report that device has been degaussed.

9.6 Users

- Users must ensure that electronic storage devices assigned to them are sanitized, by contacting their CSL, before the electronic storage device is being disposed of, transferred, returned to manufacturer, donated or surplussed.

9.7 Supporting Computer Organization

- Sanitize all servers under their control being disposed of, transferred, returned to manufacturer, donated or surplussed as outlined in this document.
- * Verify and certify the sanitization process for servers under their control, as outlined in this document, by signing the software erasure report or degaussing form for electronic storage device being disposed of, returned to manufacturer, donated or surplussed.
- * File one copy of the software erasure report or the degaussing form and attach the original to the sanitized server.

* 9.8 Computer & Communication Warehouse Unit

- * Before accepting any computer ensures that the software erasure report or the degaussing form is attached and signed by the CSL or his/her authorized representative. Archive the software erasure report or the degaussing form.
- Conduct periodic random checks of returned computers and electronic storage devices to ensure adherence to this policy.
- If it is determined that a computer or electronic storage devices still contains software or data, the department head of the sending department must be notified and the machine/device put aside in a secure location for special processing.
- Collect Bulk electronic storage devices marked for destruction and store in a secure area. Ensure that the Bulk electronic storage devices are destroyed as outlined in Section 7.

10 Violations

If it is suspected that the proper procedures as outlined in this General Instruction for the Sanitization and Disposal of Saudi Aramco electronic storage devices have not or are not being followed, the CSL must report it to the concerned department and CSA at http://csa. If improperly sanitized electronic storage devices are found it must be returned to the department having the previous custody/ownership of these storage devices.

Any user found to have violated this GI may be subject to disciplinary action, including termination of employment, referral to law enforcement agencies or other appropriate administrative or legal action.

APPROVAL

Date: __________ Recommended By: ______________________________
Administrator,
Information Protection Management Division

** Date: __________ Recommended By: ______________________________
Manager,
Information Protection & Technology Planning Dept.

* Date:________________ Approved By: ________________________________
Executive Director,
Information Technology

Digital Records Destruction Request Form

(02/10) Front Issued by: Information Protection Management Division Tel: +966-3-872-8725

Section (A) Request General Information

Request Date:	Action Requested:	Pre-action Requested:
/ /	□ Physical Destruction	□ Overwriting □ Degaussing

Section (B) Requester Contact Information

Name (Last, First Mid Initial)	Telephone #	Fax #	E-Mail Address
Building	Location		Room/ Cubicle

Section (C) Proponent Information

Proponent Approval Authority: **Name:**	**Title:**	**Badge #**	**Signature:**	**Date:** / /

Section (D) Electronic Storage Device/Media Description

#	Description	Sanitized (Yes/No)	Data Classification	Qty	Range	
					From	To
❶						
❷						
❸						
❹						
❺						
❻						
❼						
❽						
❾						
❿						

Classification of Data:	PI = Public Information	GU = General Use	RI = Restricted Information	CI = Confidential Information	GC = Government Confidential

Section (F) Action/s Taken

□ Information Protection Management Division certifies that the destruction of the items was completed successfully.

□ Canceled, explain: ....

□ Other, explain: ....

IPMD Representative: **Name:**	**Badge #**	**Signature:**	**Date:** / /

Section (F) Witnesses

Proponent's Representative: **Name:**	**Organization:**	**Badge #**	**Signature:**	**Date:** / /
Witness 1: **Name:**	**Organization:**	**Badge #**	**Signature:**	**Date:** / /
Witness 2: **Name:**	**Organization:**	**Badge #**	**Signature:**	**Date:** / /

DISTRIBUTION: Original – C&CWU	1st Copy – CSL