REVISION HISTORY

No	Date	Name	Designation	Role	Description	Version
1	01/02/2012	Hemant Nakti	IT Infra Manager	Creator	First Release	1
2	01/03/201	Vishal Doctor	Director	Approver	First Release	1
3	29/09/2014	Dinesh Rao	VP – IT & OPS	Reviewer	Review & Changes (Details of changes in Appendix 'A')	2
4	30/09/2014	Vishal Doctor	Director	Approver	Review & Changes (Details of changes in Appendix 'A')	2
5	22/01/2016	Bhavin Bheda	IT Infra Manager	Creator	Third Release	3

INDEX

Ref: ISPOL-01 IT Assets Management

Purpose:

To provide set of activities to create, store, use and destroy assets in a secure manner

Reference Document:
IT Requisition Form and Asset Deployment Receipt.

1. **Information Assets:**

1.1. Creation :

1.1.1. Information assets are created by the Branch Manager, Department Head and peer people in other department.
1.1.2. The creator of the assets is usually owner of the asset.
1.1.3. With respect to client information asset, the owner within the Organization will be the VP – IT.

1.2. Storage:

1.2.1. All information assets will be stored in server
1.2.2. The senior management will take backup of the mails and critical data in hard disk of the respective system.
1.2.3. The System Administrator will take backup on magnetic Tape, CD or other such media.
1.2.4. Users can read/write/modify information only their departmental folder

1.3. Transmission/Movement:

1.3.1. Only authorized personal or owner of the asset is allowed to transmit/move the information asset from one location to other.
1.3.2. The relocation of the information asset should be informed to all concerned.

1.4. Disposal:

1.4.1. Information assets can be deleted from the working folders once their backup is taken.
1.4.2. The information assets from the backup may be deleted once the retention period for the same is over.
1.4.3. Prior to deletion list out the details of the folder those have crossed retention stage and get the approval of the Senior Management.

2. Hardware Assets

2.1. Procurement:

2.1.1. Refer IT Requisition form.

2.2. Storage & Movement:

2.2.1. New hardware assets that are not in use should be under lock and key.

2.2.2. Hardware that store critical information should be in secure area under additional physical access control.

2.2.3. Standard hardware e.g. Desktop PC, Printer related items may move to other location within the Organization.

2.2.4. Asset Inventory should be updated once the assets movement has completed.

2.2.5. Assets like servers etc should not be moved without prior permission from the VP-IT.

2.2.6. For issue new hardware asset for use by employee, refer asset deployment receipt.

2.2.7. Problematic assets it can be replaced with duly approved by Department Head.

2.3. Installation:

2.3.1. System Administrator/Desktop Engineer will setup and installed all new hardware OR the vendor himself will setup and installed.

2.3.2. Exception can be few plug and play kind of hardware where end user can also do with help of System Administrator/Desktop Engineer.

2.4. Maintenance/Operations:

2.4.1. System administrator/Desktop engineer will do the maintenance of the hardware OR the vendor himself will do the maintenance.

2.4.2. By default, only the owner of the asset can operate the hardware.

2.4.3. Other can operate the hardware only in the presence of the owner or owner's superior.

2.5. Disposal:

2.5.1. Disposal will be done only after prior permission from the senior management.

2.5.2. Where disposal is by means of sale to third party, all information from the hardware has to be permanently deleted by formatting the hard disk or other storage media of the equipment.

2.5.3. Where disposal is by mean of physical destruction it has to be ensure that the equipment or item is permanently destroyed in a safe manner.

2.5.4. When destruction of equipment happen offsite, all information will be permanently deleted before the equipment out or will be personally accompanied and destruction supervised by Manager IT.

3. **Software Assets**

3.1. Procurement:

3.1.1. Refer IT Requisition form.

3.2. Installation:

3.2.1. System Administrator / Desktop Engineer will do the installation of the software OR the vendor himself will do the same.

3.3. Maintenance & Operation:

3.3.1. With respect to purchase software no modification should be made to the source code.

3.3.2. With respect to open source software modification to the application can be effected within the terms and condition.

3.3.3. Change to application software developed in house will be initiated by VP-IT.

3.3.4. Owner of the software can operate the software.

3.3.5. Other can operate the database only through an application interface.

3.4. Disposal:

3.4.1. Software can no longer in use can be uninstalled.

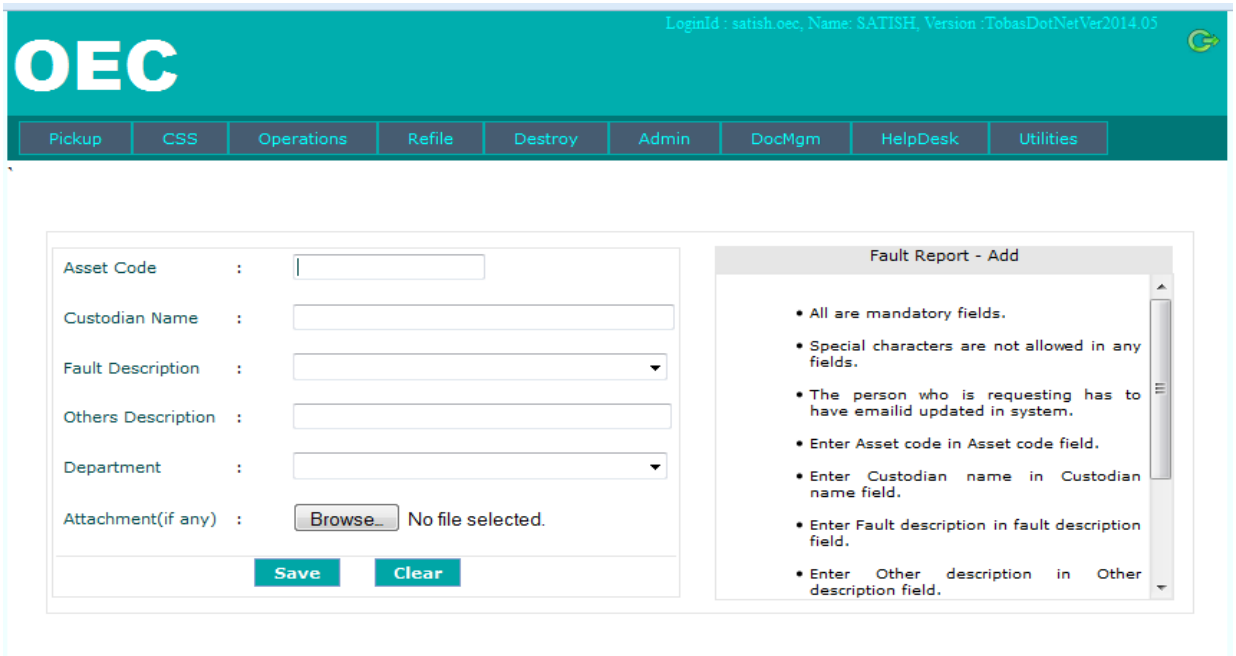
3.4.2. The physical Installation media may be retained as per the retention guideline after retention period is over the physical installation media may be disposed.

Ref: ISPOL-02 Log a fault Calls

Purpose:
The procedure lists the set of activities that are involved log a fault reports to maintain track of all fault reports and provide resolution basis request id.

Procedure:

1. **Log a Fault Report:**
   - **1.1** Enter the helpdesk link http://192.168.41.12/tobasdotnet/Login.aspx in your browser.
   - **1.2** Enter your own individual credential
   - **1.3** Click on HelpDesk menu, in that
   - **1.4** Click on Fault Report; you will view below window to fill.



   - **1.5** Asset Code : <Label which sticks on your Laptop/Computer>
   - **1.6** Custodian Name: <User of Laptop/Desktop>
   - **1.7** Fault Description: <use standard fault list>
   - **1.8** Other Description: <describe the fault details OR If the fault is not found in standard list>
   - **1.9** Department: < use drop down list to select department>
   - **1.10** Attachment (of any) : <If you have error screen shot of fault, kindly attached the error screen shot>
   - **1.11** After providing all above information click on save button; you will get request id e.g. "REQ0000022"

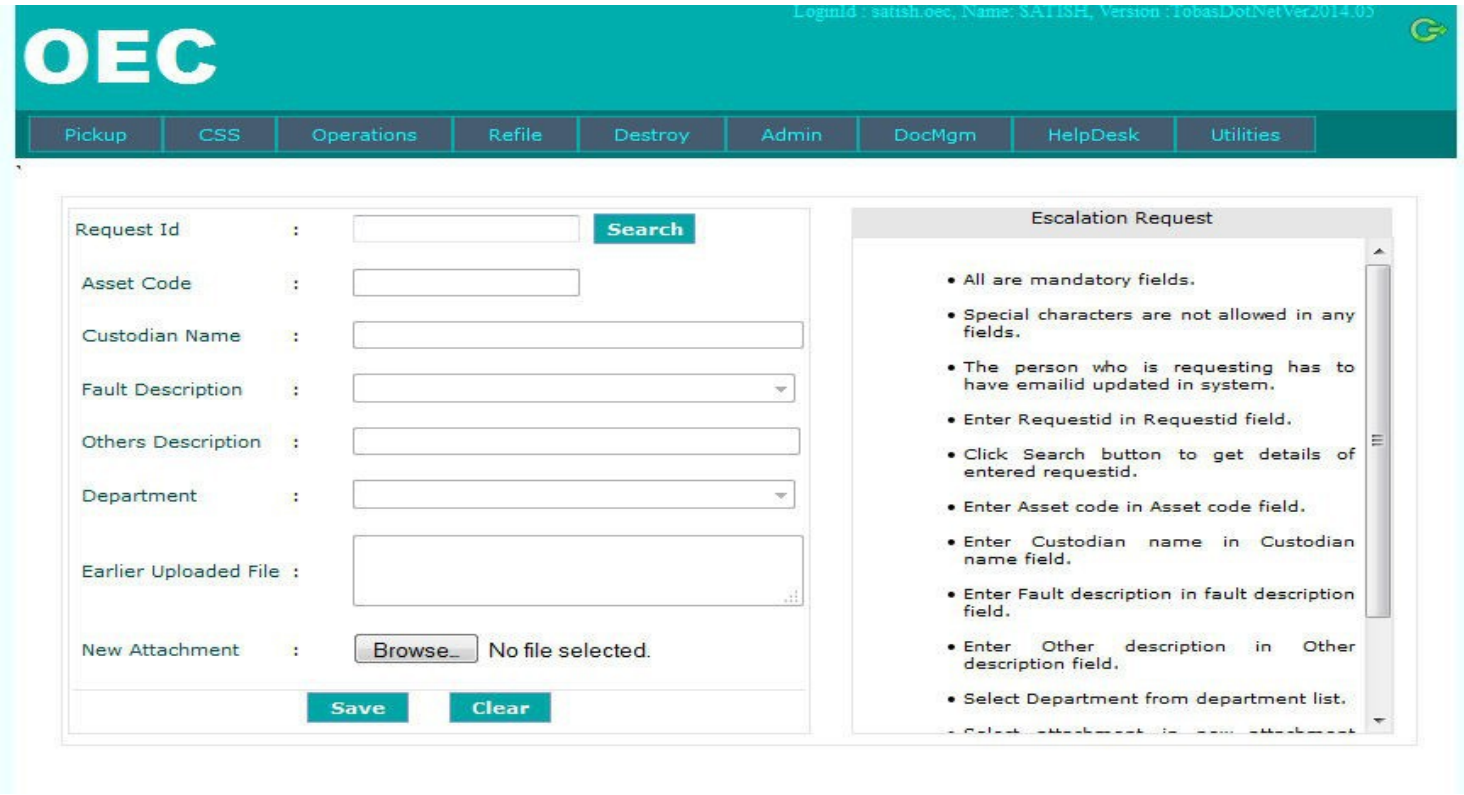
After log a fault on helpdesk the Techsupport Team will come back to you in 2 working hours, if the call gets logged before 4 pm, otherwise next business day. And resolution will be in 8 working hours.

If you not get resolution in 8 hours then you can escalate the request to next Level-2.

2. Escalate Fault Report:

2.1 Follow above steps 1.1 to 1.3

2.2 Click on Escalation Report; you will view below window



2.3 Request ID: <which you received when you logged a report first time>

2.4 Click on Search button; you will view all the details which you mentioned earlier

2.5 You need to click on save button you will view message <Request ID update successfully.> automatically the mail will received on Lelvel-2 mailbox.

Escalation Matrix:

Level-1: techsupport@oecrecords.com
Level-1: bhavin.bheda@oecrecords.com
Level-2: dinesh.rao@oecrecords.com

Ref: ISPOL-03 Backup Procedure for Data File and Database

Procedure:
To create adequate and periodic backup for electronics data generated in the Business Operations through company.

Reference Documents:

1. Data Recovery Requisition form
2. Backup & Restoration log Register.

Abbreviation:

1. RRE: Requester for Restoration
2. SA: System Administrator
3. SM: Senior Management
4. DRRF: Data Recovery
5. Requisition Form FH: Functional head
6. SH: Security Head

Description:

1. **Backup & Storage:**
   - 1.1. Identify the list of items (Database, Program, Images, Files & Folders) to be backup ongoing basis.
   - 1.2. Segregate the items on the basis if those that have to be backed up daily and those that can be backed up weekly.
   - 1.3. Using special backup server arrange automatic fix time backup of all database in to backup suitable backup device.
   - 1.4. The backup data should be stored at offsite location on daily basis and a register of In Out log of backup media shall be maintained.
   - 1.5. And accordingly update the backup logs register.

2. Restore:

2.1. Fill up the Data Recovery Requisition form.

2.2. Get approval from the concerned Function Head for the Restoration of the requested data.

2.3. Once have approval in place System Administrator will check the period to which the folder related.

2.4. If the folder is available in the local server & storage server, System Administrator will copy the data into the folder indicated in the Data Recovery Requisition Form.

2.5. If the folder or file is not available in the local server, identify the Tape in which the requested data is available.

2.6. Accordingly will bring the tape from the offsite location.

2.7. Retrieve the requested data from the Tape and copy the data into the folder indicated in the Data Recovery Requisition form.

2.8. Update the Restore log.

2.9. Inform the Person from whom the Data Recovery Requisite Form is rest as soon as the backup data is install

3. Offsite Location:

3.1. Make sure the off-site location for storage of backup data media is safe and secure.

3.2. Fill up the In Out log in register

3.3. Get approval from Security Head

3.4. Bring the Tape to the offsite location through Senior Management

3.4.1. Below mention management bands are responsible for offsite location;

1. Executive Board
2. VP's

4. Periodically Testing:

4.1. Bring the Tape from the Offsite location

4.2. Retrieve the data from the Tape

Ref: ISPOL-04 Securing - Issuing CD & DVD to Customer/Vendor

Procedure:
To ensure that the data being supplied to the customer/vendor in CD or DVD are secured, and controlled.

Reference Documents:

1. CD or DVD Writing Form.

Description:

1. At present when customers order for the supply of Data and Images of their Documents, the imaging department processes this requirement and supplies the media with the captured data back to the customers. This Involves Data Entry and Scanning process with a need to prepare the clubbed final Data as per customer format.
2. It is essential that in this process there has to be a strict control as to eliminate mix up or wrong databases get merged, and sent to wrong hands, by human error.
3. Through this process OEC introduce double checking and independent verification of the Data or Images-files being written to CD or DVD media before getting shipped out of OEC.
4. The Imaging Department Supervisor after conducting QC checks of images files (Quality Correctness, and Completeness of Data) shall use the data entry file created for the same customer to merge and link the image-files using software tool.
5. At this stage Supervisor shall prepare a document form (CD or DVD Writing Form) mentioning following information:
    - Customer Name & Vendor Name
    - Department
    - Brief of Data / Work Order Number / Volume Number of the batch (Depends on Customer Instruction)
    - No of files Indexed as per Data entry mage (Bar-coded)
    - No of Image file captured in the scanning process
    - Label of CD/ DVD
    - Total Number of the CD/DVD used for the preparation of this data files.
    - Data Location stored in Server, Hard Disk, Pen Drive
    - Requested by (Name, Signature & Date)
    - Approved by (Name, Signature & Date)
    - Verify by (Name, Signature & Date)
6. The Imaging department supervisor shall handover this CD/DVD to Techsupport Team with the form for their verification and certification.
7. And any other departments can also share/handover the Data, Form & Media to Techsupport Team to write the Data on those Media for customer use.
8. Techsupport shall check the relevance of the customer order and Data so captured for its completeness and sign in the form as authorized for delivery.
9. Techsupport will then handover the CD/DVD to requester for delivering to the customer.
10. Also each CD/DVD shall have a proper label on the media cover giving the Customer Name.

Ref: ISPOL-05 Access Management

Purpose:
The procedure lists the set of activities that are involved in the creation and maintenance of user ids and password.

To provide instructions for activities that involve restriction of access at the network, email, IM and application levels by means of user ids and passwords.

Description:

1. **System & Network ID Creation:**
   1.1. When a new employee joins, HR sends a request to Techsupport Team with the relevant Department Head's approval for creating a user Id to access OEC's system.
   1.2. The request is sent through the "User ID creation log".
   1.3. Once the required id is created, the System Administrator will configure the id on his/her PC or Laptop.
   1.4. As soon as the Employee resigns or is terminated, HR sends a request to Techsupport Team with the Department Head's approval for Deleting the relevant user Id to restrict system access.
   1.5. The request will be send through the "User ID Deletion log".
   1.6. As soon as the Id has been deleted Techsupport Team will confirm to HR.
   1.7. In case existing ID's re allocation, HR Sends a request to Techsupport Team with the relevant Department Head's approval.

2. **User ID for Network Access:**
   2.1. Create Individual user ids and passwords for employees.
   2.2. Allocate an individual user id and password to each employee, depending on their role and the level of access required.
   2.3. System access is controlled by means of physical access and logical access controls.
   2.4. Ensure the user is changing his/her password frequently or fix automatic password expiry dates for employees.
   2.5. Fix the respective access to folders for the user id in consultation with Department Heads.

3. **User ID for Application Access:**
   3.1. Create a separate user id and password that is unique for each user of the application.
   3.2. The restriction to using applications is based on the Application user id and password alone.
   3.3. Intimate the user id and password to the respective users.
   3.4. The restriction to using applications is based on the Application user id and password alone.

4. **User ID for Internet Access:**
   4.1. Create a separate user id and password that is unique for each user.
   4.2. Ensure the user is changing the password frequently or fix automatic password expiry dates for employees.
   4.3. Allow access to the Internet for the Employee in consultation with the Department Head.

5. **Email ID for Mailbox Access:**
   5.1. Create separate unique email id and password for the user after the Department Head's approval.

5.2. Individual e-mail id will be created in the below format; firstname.surname@oecrecords.com and generic e-mail id will be departmentname@oecrecords.com

6. **Others:**
   6.1. The passwords are changed at regular intervals.
   6.2. User can change their password once they receive the intimation.
   6.3. IM and Mailbox password will be shared with users after Department Head approval.
   6.4. Conduct review of the user id's and passwords allotted to the users to check for compromise of password and/or access restrictions.

7. **Privilege Access:**
   7.1. The privilege access is allocated based on type of the Project/Application/Role in the organization

Ref: ISPOL-06 Network Management

Purpose:
This procedure is meant to ensure the availability and security of the shared network resources which support the processing mission of the OEC and the administrative activities that underpin this mission. This procedure supplement and clarify the principles set out in the OEC Policies as they apply to the OEC centrally managed network infrastructure and the operation of systems therein.

Description:
Any type of computer system, network equipment, or other device which operates on the OEC network infrastructure, includes personal computers, servers, network-enabled printers, network hubs or switches, and any other device which uses the network should be managed and documented.

The OEC-owned network infrastructure is managed by the Tech Team. This includes the OEC network backbone and network devices.

System Administrators follow existing recommended practices and/or standards for configuration and operation of equipment where these are available.

System Administrators should apply relevant security patches in a regular and timely fashion as well as running up-to-date anti-virus software where applicable.

Before operating a system on the network, the logical placement of the system within the network should be decided in consultation with the management according to the function and sensitivity of the system.

The tech Team will monitor bandwidth performance and the types of inbound and outbound network traffic permitted through the Internet gateway and other points within the OEC network.

Use of OEC Network connections to host services for unauthorized commercial purposes is not allowed.

The Tech Team will assign IP addresses to networked systems either at system installation time. Using or attempting to use a different IP address than the one assigned is not allowed without formal authorization process.

Operation of network-authoritative services (DNS and routing-related services) is not allowed without authorization by Management.

Interfering or attempting to interfere with the normal operation of networks and systems within or external to the OEC should not be allowed. Examples of this type of abuse include unreasonable use of resources, scanning, monitoring, interception, impersonation, or modification of systems or data without authorization or consent of the system or data owner.

Use or transmission of malicious software such as computer viruses which could provide unauthorized access and/or infect systems should not be allowed. Computers infected with malicious software will be considered as a security compromise.

Use of the OEC Network must not violate the OEC Policies. Such violations include copyright, distribution of computer viruses or other malicious programs, unauthorized access, or other unlawful use as described in the policies.

Systems operating in violation of law; these procedures; or which pose a risk to the security, integrity, or availability of systems or the OEC Network will be disconnected from the network by Tech Team upon confirmation and approval from IT VP.

Ref: ISPOL-07 Desktop Computer and Laptop Installation

Purpose:
Standardized secure installation and maintenance of Computer Hardware & Software

Also this information is to be used when a user requests the addition or reconfiguration of a computer on OEC network

Description:

1. **Setup New Computer/Laptop:**

1.1. Installed Operating System (If applicable)
1.2. Set Time Zone setting (GMT +05:30) and Date format will be dd/mm/yyyy
1.3. Create two NTFS partition e.g. C(OS) drive and D(Data) drive
1.4. Check vendor website for latest downloads, drivers, BIOS, etc. for machine model.
1.5. Rename computer name e.g. (For Laptop OECNMLP001 and for Desktop OECNMDT001). check Active Directory Computer list to avoid duplications (If applicable)
1.6. Move computer on domain (If applicable)
1.7. Set Password for Administrator account
1.8. Create Adminoec account in user with administrator privileges
1.9. Create Username (Name<space>Surname) with limited privileges in user with password.
1.10. Configure Network setting on DHCP mode for Laptop Users
1.11. Enable Windows Firewall
1.12. Install current Service Pack for Operating System
1.13. Install all Windows Updates from windowsupdates.microsoft.com
1.14. Map Network Drive
1.15. Printer Drivers Installation
1.16. Add TOBAS. Net link in Browser favorite
1.17. Add ERP Link in Browser favorite
1.18. Install Adobe Reader
1.19. Install PDF Writer Printer
1.20. Install WinZip / WINRAR (If applicable)
1.21. Install MS Office (If applicable)
1.22. Configure Email Client with standard Signature format (If applicable)
1.23. Configure Email data path in D drive (If applicable)
1.24. Skype Messenger (If applicable)
1.25. IP Messenger (If applicable)
1.26. VPN Client (If applicable)
1.27. Citrix Online Plug-in Web (If applicable)
1.28. Installed approved software's

2. Inventories:

2.1. Tech Team will note down the Part Number, Model & Serial Number and accordingly update the IT Asset Inventory (If Computer/Laptop is newly purchased)
2.2. Asset Name, Workgroup, System login name and network details (If applicable)
2.3. Installed software which will not installed by default

3. Backup of current data (If applicable):

3.1. Browser favorites & Bookmarks
3.2. Mail Data e.g. Pst's, dbx, .eml & .nk2
3.3. Email ID Address Book
3.4. Folders & Files (End user needs to share the list of folder and files which needs to backed up)

4. Hardening:

4.1. Configure password for BIOS
4.2. Disable Floppy drive (If applicable)
4.3. Disable CD-R/W drive (If applicable)
4.4. Disable USB Mass storage port (If applicable)
4.5. Disable Guest Account
4.6. Un installation games
4.7. Enable require services
4.8. Disable remote desktop option
4.9. Turn off System Restore setting

5. Ensure the task before leaving the installation/re configuration area:

5.1. Files and folder were restored
5.2. Found their Internet favorites and bookmark
5.3. Found mapped drive
5.4. Able to print document through require printers
5.5. Found and open previously save documents
5.6. Able to save new documents
5.7. Test scanner and any other attached hardware and all is functioning properly
5.8. Able to Send/Received Emails
5.9. Able to access old mails
5.10. Able to access all applications used on a regular basis
5.11. Test requested and approved software functions
5.12. Speaker and sound functionality

Appendix – A

#	Date	Procedure Name	Brief description about the changes incorporated
1	15 Sep 2014	Information Security Procedures	1. Consolidated individual procedures listed in Ver. 1.00 into an integrated version 2.00.
2	22.01.2016	Information Security Procedures	3. Matrix updated with the email id of Mr. Bhavin Bheda.

DEPARTMENT		ISSUE DATE	REVISION #
ITD	**OEC-ITD-IS-P-02**	**2016-01-22**	**3.0**
	INFORMATION SECURITY PROCEDURES		PAGES **18** of 18