# CNH Warranty Audit

## Ibcos Policies and Procedures

**Version 0.1**

**January 2024**

## CONTENTS

## OVERVIEW

For CNH Warranty Audit purposes, all Dealers must ensure they comply with the following requirements:

- Have High Security Passwords turned on for Gold
- Have the System Audit turned on in Gold
- Implement the New Starter Process
- Implement the User Access Permission Process
- Implement the Leaver Process
- Carry out regular user and access reviews

You can find instructions for all these requirements in this document.

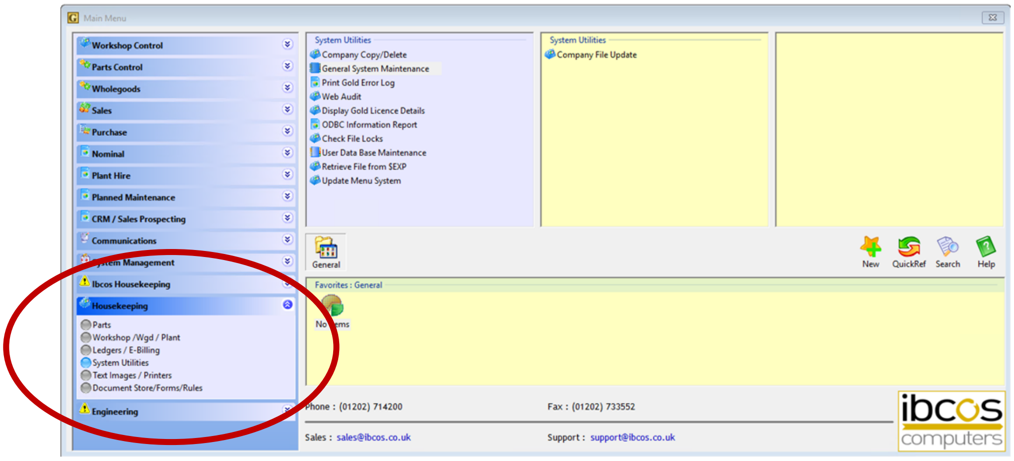
### HOW TO TURN ON HIGH SECURITY PASSWORDS

All Dealers must have their security password set to high. This setting will enforce the following rules:

- Users must enter both their initials and a password to be able log into Gold.
- Passwords will contain 6 characters with at least 1 number.
- Users will be forced to change their passwords every 30 - 90 days.

**Important Note:** Once the password security has been set to High, it cannot be reverted back to a lower security setting.

To set High Security for your system, access to the Housekeeping menu is required.



When you first set the password security to High, users will be asked to enter their initials as well as their current password when they log in. They will only be asked to change this again once the timeframe for changing the password has elapsed.

For example: if you set the password to be changed every 90 days, then the user will be asked to enter their initials and their current password for the first 90 days. After 90 days, the user will be prompted to create a new password.

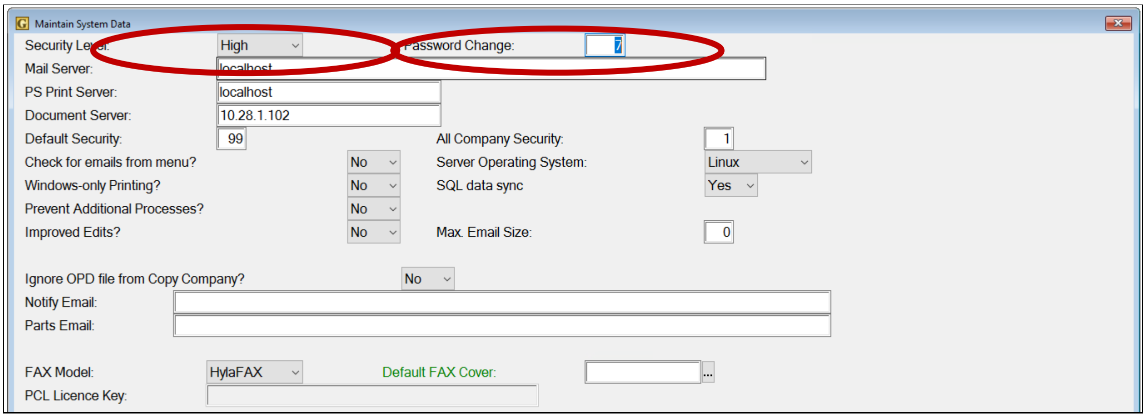
When you first set the password security to High, you must set the initial number of days on the ‘Password Change’ field to ‘7’. After 7 days users will be prompted to create a new password which will meet the high security requirements.

After 7 days, you must then go back into the General System Maintenance screen and set the ‘Password Change’ field to either 30, 60 or 90 days as required.

It is recommended to inform all users before turning on High Security.

## Step 1

- Ask all users to log off the system
- Select the Housekeeping Menu (if you are using Classic Gold, this is part of the System Management menu)
- Select ‘System Utilities’
- Select ‘General System Maintenance’
- Set the ‘Security Level Field’ to ‘High’
- In the ‘Password Change’ field, set the number of days to force a password change to 7
- Select ‘OK’ to save



Maintain System Data

Security Level: High
Password Change: 7
Mail Server: localhost
PS Print Server: localhost
Document Server: 10.28.1.102
Default Security: 99
All Company Security: 1
Check for emails from menu? No
Server Operating System: Linux
Windows-only Printing? No
SQL data sync Yes
Prevent Additional Processes? No
Improved Edits? No
Max. Email Size: 0
Ignore OPD file from Copy Company? No
Notify Email:
Parts Email:
FAX Model: HylaFAX
Default FAX Cover:
PCL Licence Key:

All users will now be forced to enter both their initials and their current password when they log in.

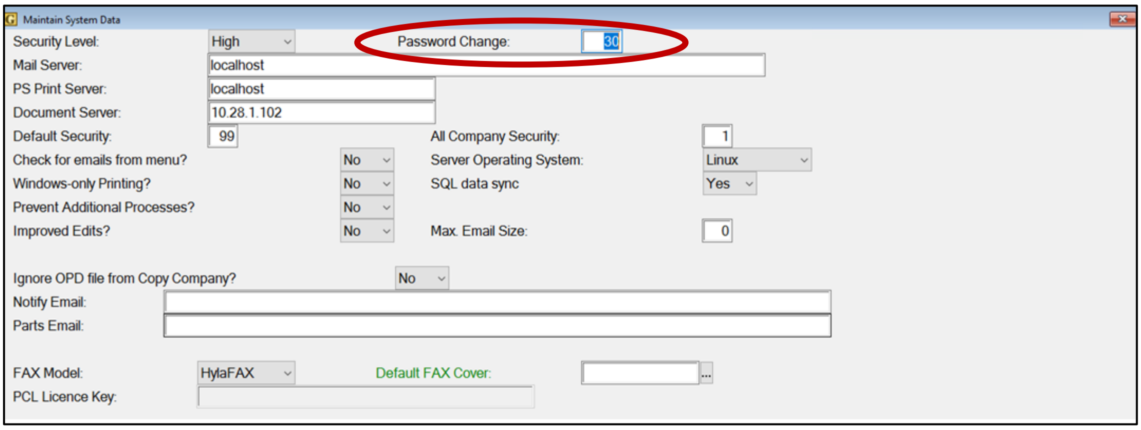
After 7 days users will be prompted to create a new secure password which will meet the high security requirements. See the section on “User Setting” below.

## Step 2 (7 days later)

When users have had time to log in and to change their password to a more secure password the number of days for password change can be increased.

- Ask all users to log off the system
- Select the Housekeeping Menu (if using Classic Gold, this is part of the System Management menu)
- Select ‘System Utilities’
- Select ‘General System Maintenance’
- Set the ‘Security Level Field’ to ‘High’

- In the ‘Password Change’ field, set the number of days to force a password change to between 30-90 days



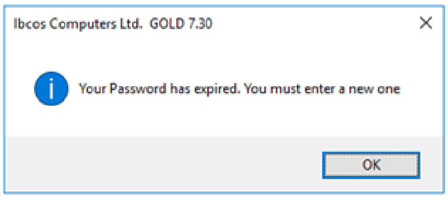
Maintain System Data

Security Level: High
Password Change: 30
Mail Server: localhost
PS Print Server: localhost
Document Server: 10.28.1.102
Default Security: 99
All Company Security: 1
Check for emails from menu? No
Server Operating System: Linux
Windows-only Printing? No
SQL data sync: Yes
Prevent Additional Processes? No
Improved Edits? No
Max. Email Size: 0
Ignore OPD file from Copy Company? No
Notify Email:
Parts Email:
FAX Model: HylaFAX
Default FAX Cover:
PCL Licence Key:

This setting will ensure all users reset their password every 30-90 days (depending on the number of days entered).

## User View

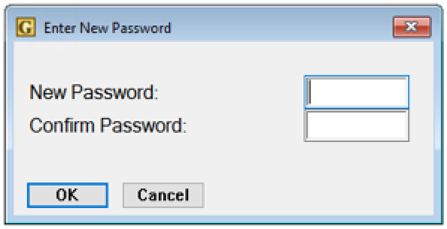
After 7 days, each user will receive a notification to tell them their password has expired, and they must enter a new one:



Ibcos Computers Ltd. GOLD 7.30

Your Password has expired. You must enter a new one

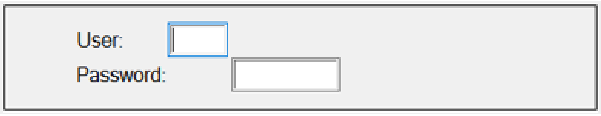
Press the ‘OK button and enter a new password. Please note: this password must be 6 characters long and contain at least 1 number.



Enter New Password

New Password:
Confirm Password:

Every time a user logs in after setting their new password, they will be asked to enter their initials and new password.



User:
Password:

This process will reoccur each time the number of days in the password reset field is reached, e.g., every 90 days.

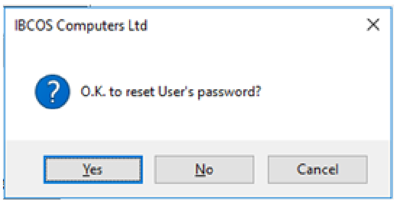
## How to reset a user’s password

Please note, with the high security setting, Administrators will no longer be able to view user passwords.

If a user has forgotten their password, or is unable to log in, a temporary password can be issued, after which they will be prompted to create a new one.

- Go to System Management
- Select ‘Security’
- Select ‘Personnel Security File’
- Enter the user’s initials
- On the ‘Details Tab’ select ‘New Pwd’

A pop up will appear asking if you want to reset the user’s password:



IBCOS Computers Ltd

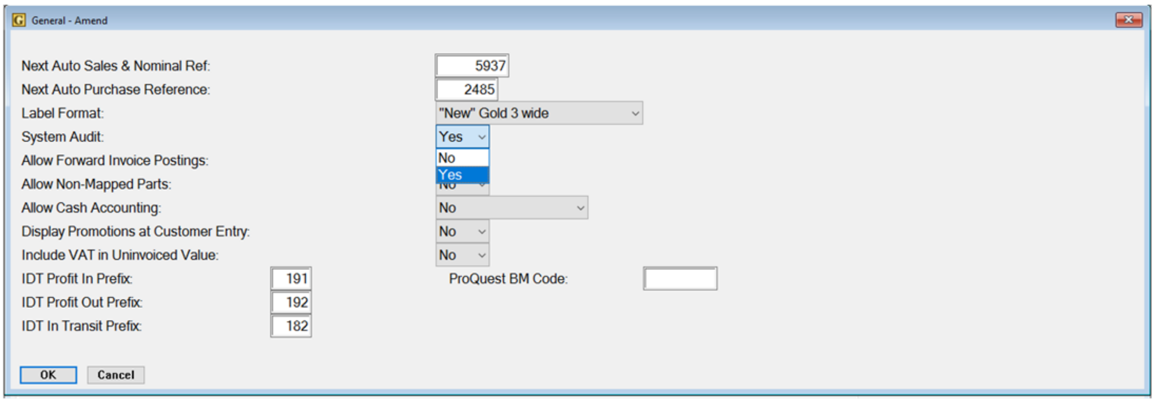
O.K. to reset User's password?

Select ‘Yes’, and a temporary password will be issued to give to the user. This temporary password must be changed when the user next logs on.

## HOW TO TURN ON THE SYSTEM AUDIT

The System Audit should always be turned on. Turn on the system audit by following these steps:

- Ask all users to log off the system
- Go into ‘System Management’
- Select the ‘Company Control File’
- Select ‘Amend’
- Move across to the ‘Accounts Tab’ (in Classic Gold, do this by pressing F12)
- Select ‘General’
- Set the ‘System Audit’ field to ‘Yes’
- Press F2, and select ‘Yes’ to save changes



General - Amend

| | | | |
|---|---|---|---|
| Next Auto Sales & Nominal Ref: | 5937 | | |
| Next Auto Purchase Reference: | 2485 | | |
| Label Format: | "New" Gold 3 wide | | |
| System Audit: | Yes | | |
| Allow Forward Invoice Postings: | | | |
| Allow Non-Mapped Parts: | No | | |
| Allow Cash Accounting: | No | | |
| Display Promotions at Customer Entry: | No | | |
| Include VAT in Uninvoiced Value: | No | | |
| IDT Profit In Prefix: | 191 | ProQuest BM Code: | |
| IDT Profit Out Prefix: | 192 | | |
| IDT In Transit Prefix: | 182 | | |

## How to run a check to see if users have accessed a program to edit data

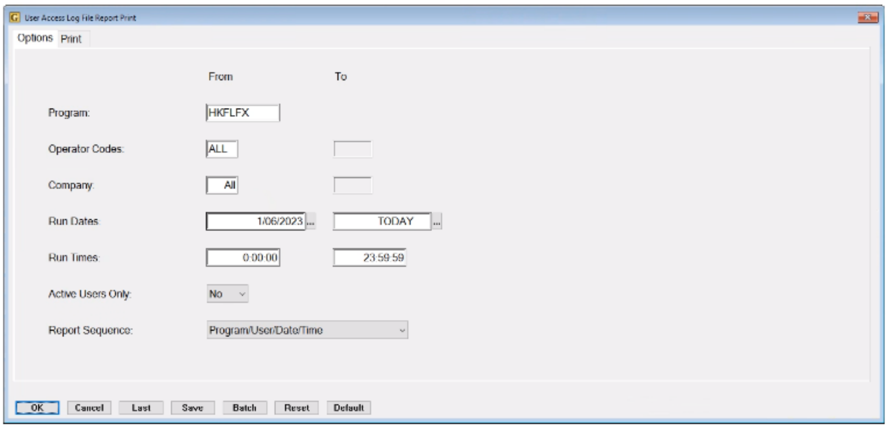
Gold data is held in data files called ISAM files.

The only way to manipulate data in the data files is via programs that are held on the Ibcos only housekeeping menu which requires a password from Ibcos to access.

This document explains how to run a report to show if any user has accessed a program that could alter the data in the files.

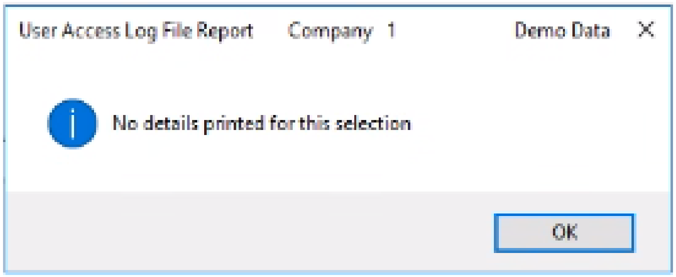
## How to check if users have accessed the Find / Replace Data in ISAM Files program

- Go into ‘System Management’
- Select ‘Utilities’
- Select ‘Print User Access Log Details’
- Select the program ‘HKFLFX’
- Enter the date range you want to review
- Press ‘Enter’



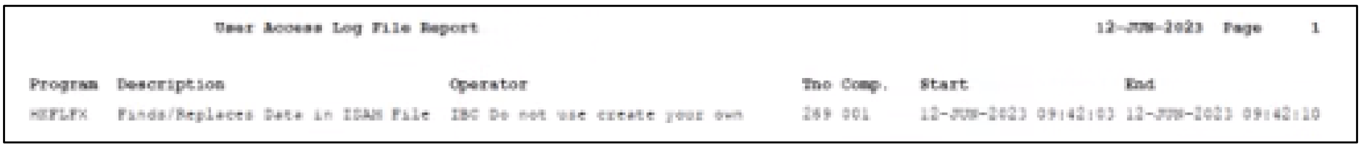
| | From | To |
|---|---|---|
| Program: | HKFLFX | |
| Operator Codes: | ALL | |
| Company: | All | |
| Run Dates: | 1/06/2023 | TODAY |
| Run Times: | 0:00:00 | 23:59:59 |
| Active Users Only: | No | |
| Report Sequence: | Program/User/Date/Time | |

This should not produce any data, and you should see this pop up:


User Access Log File Report    Company 1    Demo Data

No details printed for this selection

If anyone has accessed the program, a report will be produced:

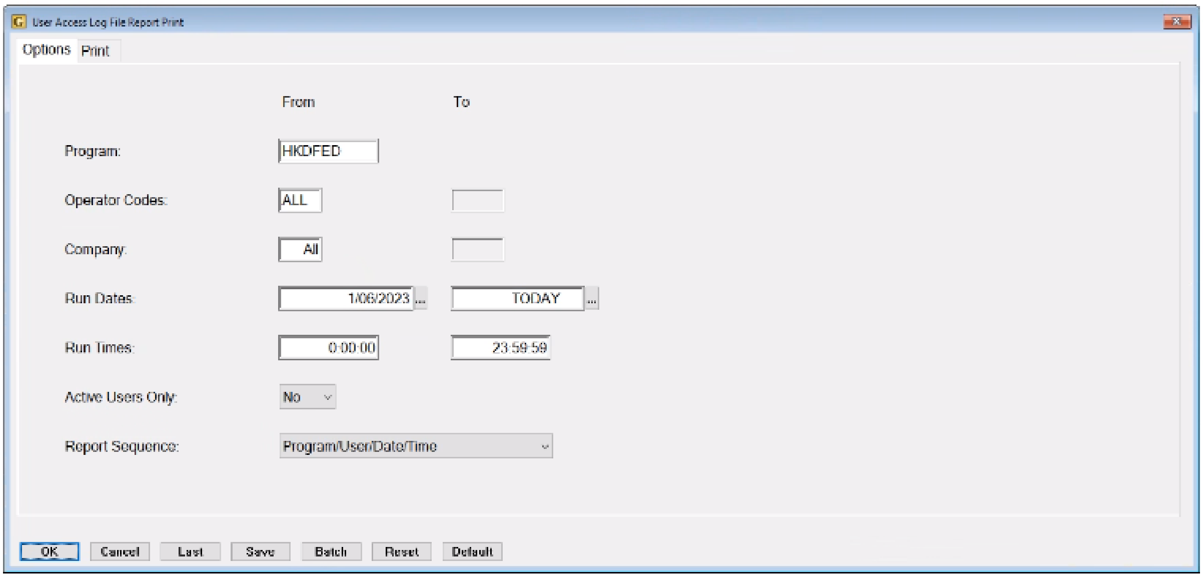


```
                   User Access Log File Report                                                          12-JUN-2023  Page      1

Program  Description                    Operator                        Tno Comp.   Start                 End
HKFLFX   Finds/Replaces Data in ISAM File  IBC Do not use create your own   269 001     12-JUN-2023 09:42:03 12-JUN-2023 09:42:10
```

## How to check if users have accessed the Edit ISAM/ADS Type Files program

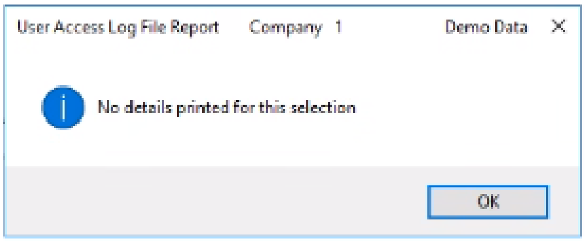
- Go into ‘System Management’
- Select ‘Utilities’
- Select ‘Print User Access Log Details’
- Select the program ‘HKDFED’
- Enter the date range you want to review
- Press ‘Enter’



User Access Log File Report Print

| | From | To |
|---|---|---|
| Program: | HKDFED | |
| Operator Codes: | ALL | |
| Company: | All | |
| Run Dates: | 1/06/2023 | TODAY |
| Run Times: | 0:00:00 | 23:59:59 |
| Active Users Only: | No | |
| Report Sequence: | Program/User/Date/Time | |

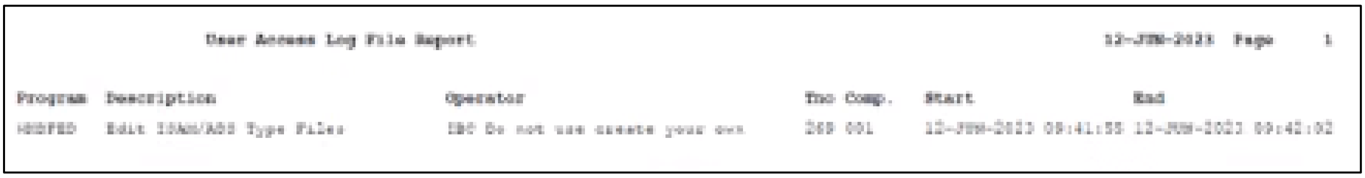
This should not produce any data, and you should see this pop up:



User Access Log File Report Company 1 Demo Data

No details printed for this selection

If anyone has accessed the program, a report will be produced:



```
                 User Access Log File Report                                                  12-JUN-2023  Page     1

Program  Description                  Operator                      Tno Comp.   Start                End
HKDFED   Edit IDAN/ADS Type Files     IBC Do not use create your own 269 001    12-JUN-2023 09:41:55 12-JUN-2023 09:42:02
```

## How to verify the reason these programs were accessed

Please contact Ibcos Support if anyone has accessed either of these programs to check the records of who accessed the program and for what reason.

Ibcos Support will have a record of any access to the data edit programs by Ibcos staff members.

## NEW STARTER PROCESS

Dealers must keep a record of all new starters, to include the following information:

- Name
- Start Date
- Job Title
- Level of Gold access they have been granted (including super user rights)

## USER ACCESS PERMISSION PROCESS

Users should be granted only the minimum access level codes required for their job role; with consideration being given to the segregation of duties where possible.

Restriction should be applied to the super user option and should only apply to users who require the following abilities:

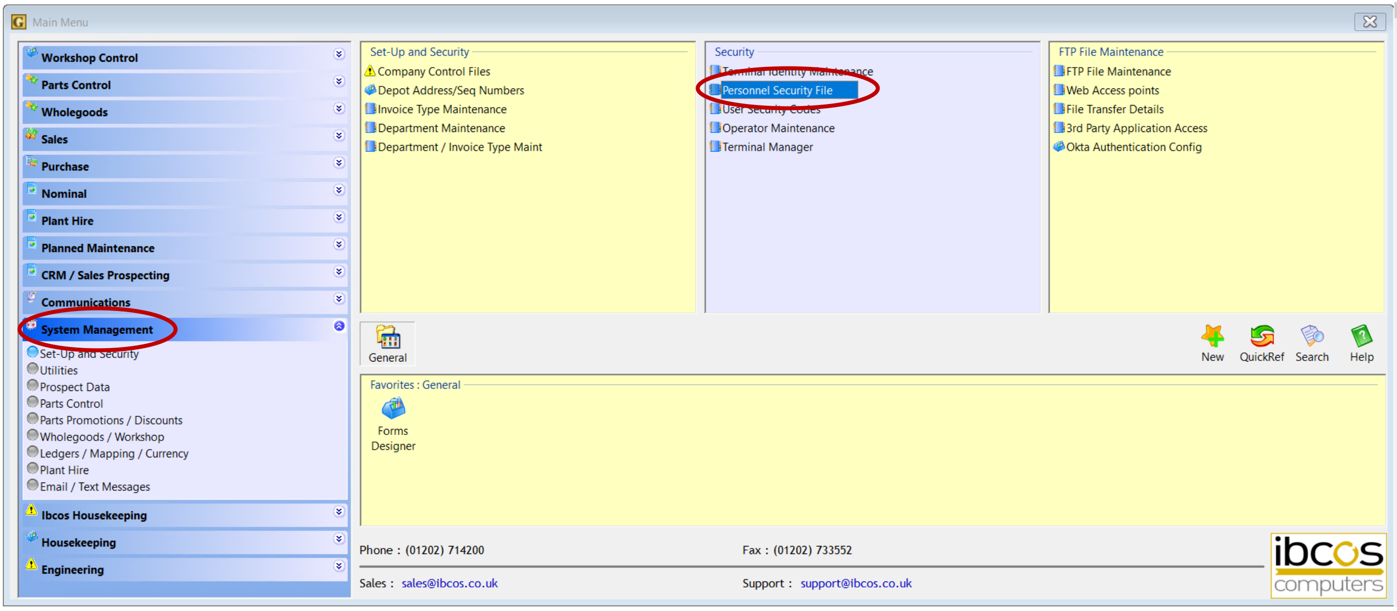
- Can log in and use the system even when locked to users.
- In "Report User Status" can lock/unlock Gold and kill other users.
- Write/Post to Archive Companies.
- Within Document Maintenance can delete a document awaiting payment authorisation.
- In Plant Equipment Maintenance may change the purchase price.
- Can change the Security setting in "General System Maintenance".
- Receive notifications when a new update is ready to be loaded.

Regular checks of each user’s access permissions in Gold should be carried out. Ibcos suggest these checks are carried out on a quarterly basis as a minimum.

## LEAVER PROCESS

When an employee leaves the company, you must mark them as a leaver in Gold to prevent them from accessing the system.

- Go into System Management - Security
- Select Personnel Security File

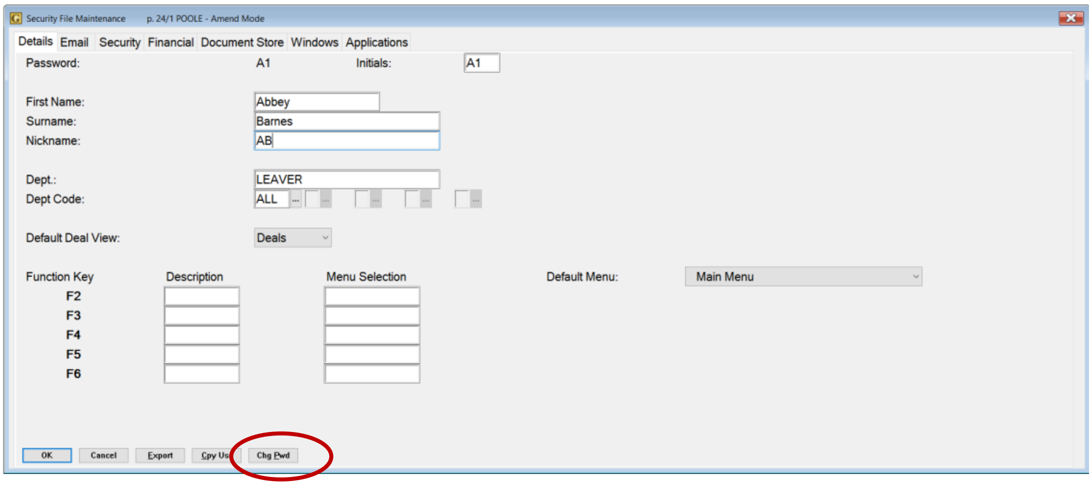


Phone : (01202) 714200 Fax : (01202) 733552

Sales : sales@ibcos.co.uk Support : support@ibcos.co.uk

- Select the user who has left the business.

- On the “Details” tab enter the word LEAVER into the Dept field then click the “Chg Pwd” button to reset the users password.



Password: A1 Initials: A1

First Name: Abbey
Surname: Barnes
Nickname: AB

Dept.: LEAVER
Dept Code: ALL

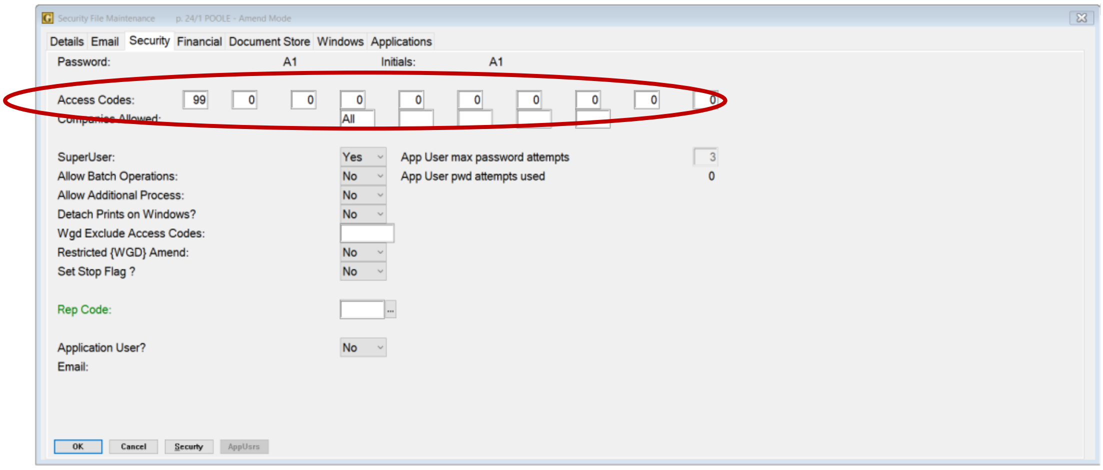
Default Deal View: Deals

| Function Key | Description | Menu Selection |
|---|---|---|
| F2 | | |
| F3 | | |
| F4 | | |
| F5 | | |
| F6 | | |

Default Menu: Main Menu

- Go to the “Security” tab

- In the Access Code section, put 99 on the first field and leave everything else as 0. Note: this step can be ignored if Access Code 99 is in use.



Password: A1 Initials: A1

Access Codes: 99 0 0 0 0 0 0 0 0 0

Companies Allowed: All

SuperUser: Yes

App User max password attempts 3

App User pwd attempts used 0

Allow Batch Operations: No

Allow Additional Process: No

Detach Prints on Windows? No

Wgd Exclude Access Codes:

Restricted {WGD} Amend: No

Set Stop Flag ? No

Rep Code:

Application User? No

Email:

- Click save and the user will no longer be able to access Gold.

**SERVER ROOT PASSWORD**
The server root password should be restricted to a minimum required number of staff and a complex password should be used to ensure security is maintained.

Unix/Linux passwords can be set as complex, but this is not mandatory.

Ibcos recommend the use of the following for the server root password:

- uppercase characters
- lowercase characters
- digits
- other characters (e.g., punctuation marks)
- a mix of the above

| Version | Date | Changes | Distribution |
|---|---|---|---|
| 1.0 | 22/01/2024 | Updated to final version ready to publish. | All CNH dealers running Ibcos Gold software |