DOCUMENT HISTORY

Document Location
This is a snapshot of an on-line document. Paper copies are valid only on the day they are printed. Refer to the author if you are in any doubt about the currency of this document.

Revision History
Date of this revision: 03 July 2006
Date of next revision: (date)

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Revision Date</th>
<th>Summary of Changes</th>
<th>Revised By</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>10-05-05</td>
<td>Draft</td>
<td>Thiagu</td>
</tr>
<tr>
<td>1.0</td>
<td>15-05-05</td>
<td>Baselined</td>
<td>Thiagu</td>
</tr>
<tr>
<td>2.1</td>
<td>15-Jun-06</td>
<td>Revised for LDAP / compare with IS</td>
<td>Nisha</td>
</tr>
<tr>
<td>2.2</td>
<td>20-Jun-06</td>
<td>Based on review comments of KG</td>
<td>Nisha</td>
</tr>
<tr>
<td>2.3</td>
<td>23-Jun-06</td>
<td>Based on review comments of Thiagu</td>
<td>Nisha</td>
</tr>
<tr>
<td>2.4</td>
<td>26-Jun-06</td>
<td>Based on comments of Elango – revised table at end</td>
<td>KG</td>
</tr>
<tr>
<td>2.5</td>
<td>03-Jul-06</td>
<td>Changed the password guidelines to give examples</td>
<td>KG</td>
</tr>
</tbody>
</table>

Approvals
This document requires following approvals. Signed approval forms are filed in the Quality section

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>(name)</td>
<td>(title)</td>
</tr>
</tbody>
</table>

Distribution
This document has been distributed to

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>HELIX portal</td>
<td>(title)</td>
</tr>
</tbody>
</table>

References
This document is based on and refers to the following documents:

<table>
<thead>
<tr>
<th>No.</th>
<th>Author</th>
<th>Title</th>
<th>Reference</th>
<th>Version no.</th>
<th>Date</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>InfoSec</td>
<td>Infosec Policy</td>
<td>HELIX portal</td>
<td>(Version no.)</td>
<td>(Date)</td>
<td>(Pages)</td>
</tr>
</tbody>
</table>
PASSWORD MANAGEMENT

1.1 GENERAL GUIDELINES FOR USERS ................................................... ................................................... 4
1.2 USER IDS CONVENTIONS: ................................................................. 4
1.3 PASSWORD POLICIES ........................................................................... 5
1.4 PASSWORD FOR NEW USERS............................................................... 6
1.5 CHANGING PASSWORD ....................................................................... 6
1.6 FORGOTTEN PASSWORD ..................................................................... 6
1.7 CHANGE SECURITY TOKEN................................................................. 7
1.8 USER PASSWORD MANAGEMENT GUIDELINES GIVEN BY INFOSEC GROUP ................................................... 8
PASSWORD MANAGEMENT

1.1 GENERAL GUIDELINES FOR USERS

- For all applications the employee id is to be used as the user id. Three digit **Ids like 976 should be entered as 0976**

- If you have forgotten your password you can use the 'Forgot Password' option explained below. But your email id should have been registered in the HRMS database by your local HR representative, for your old password to be mailed to your mail box. Once it is updated in HRMS it will be synchronized with the Helix database by the process that runs every one hour.

- The applications that will be synchronized by the 'Change Password' option provided on Helix screen are:
  - MMS
  - Help@Hexaware
  - Autolib
  - Cockpit
  - Hex!Folks
  - Ewise
  - PollVault
  - Hex::Forum
  - myBenefits
  - Time & Billing
  - Resource Management
  - HR DashBoard
  - KART

1.2 USER IDs CONVENTIONS:

The user id for all Employees shall be their Employee Ids as generated by the PeopleSoft HRMS system, and shall be treated as a character string only – if the Employee Id is a 3 digit id then the digit '0' is to be prefixed to the Employee id. In other cases the Employee id can be four or more than four characters length.

In special cases where the user is not an employee of the Company a alpha/alphanumeric string can be allowed to be the user id

Examples of UserId : 0133, 6789, 12345 , HelpDeskRep
1.3 **PASSWORD POLICIES**

The policies that are to be followed for passwords of user accounts for all the applications delivered by Internal Systems Group are listed below in compliance with InfoSec policies on Password Management.

- Password complexity is enabled.
- Password should conform to the following rules
  1) The password should be a minimum of 9 characters and max 12 characters
  2) It should have at least any three of the following four types
     1. An UPPER CASE character (A to Z)
     2. A lower case character (a to z)
     3. A numeral (0 to 9)
     4. A Special Character (!@#$%&()+={};<>,.?/|
  3) The password should include at least one alphabet and one digit as in examples: *MyWord123, Superman2006, forget(me)not*
  4) The password should NOT use the words or formats given below (irrespective of case)
     a. pass, pass123, password, password123, Hexaware, Hexaware123
     b. passNNNN, passwordNNNN or HexawareNNNN < NNNN is the employees id>
     c. Employees First Name and/or Last Name
  5) The New password should not be same as the current password.

- The default password should be changed at the time of first time login.
- All passwords are valid for a maximum period of one month.
- Maximum of 7 passwords will be remembered in history.
- Accounts associated with a password will be locked after 6 consecutive failed login attempts.
- Account lockout duration will be 30mins after which it will be automatically unlocked.
- Password change shall be forced during the first login.
- Users can change their passwords whenever necessary.
- Users can change their Security Token whenever they want.
- When passwords are reset and temporary passwords are issued to users, proper validation is carried out by confirming Date of Birth and Security token.
- System shall display warning message for users to change the password, from 15th day of last successful password change.
1.4 PASSWORD FOR NEW USERS

Any new employee id created will be given access to almost all applications immediately based on their role. Your record will be assigned a default password. To get the default password use the ‘Forgot Password’ function explained in section 1.6. After getting the password through email, you need to change it before first use as explained in section 1.5.

1.5 CHANGING PASSWORD

A menu has been provided on all pages (under User Info menu) and a link in the login page to enable changing the password by the users.

- The user is required to provide the employee id and the current password for registering a new one.
- If the current password is a default password like ‘password123’ or ‘pass’ or ‘pass2614’ (in any case), the user should provide his/her date of birth as additional proof.
- The Date of Birth provided will be validated against the data from HRMS. This is meant to ensure that your password is not changed by others.
- If the user does not have a Security token, he/she will be re-directed to the Change Token screen where user can choose a token. On creating the token, the password will be changed.
- If the user already has a Security token, the password will be changed there itself.

If the current password is not known, the user should use the ‘Forgot Password’ link or button explained below.

The new password will be stored in an encrypted form in the database. The passwords of users who changed will be synchronized to other applications like Help@Hexaware, MMS, Autolib, HexForum and EWise by the process that runs every one hour. For other applications, the new password can be used immediately.

The new password given should conform to the rules given in the previous section of this document.

1.6 FORGOTTEN PASSWORD

A menu is provided on all pages (under User Info menu) and a link in the login page to enable getting the forgotten password by the users. This is expected to almost eliminate the need for the users to approach the Internal Systems Group or STG or a system administrator to help resetting the password. The user is expected to contact ISG Help Desk ONLY when the password received using this method does not work.

- Enter your Employee id on the screen.
- Also to ensure that your password is not accessible to others, you are required to provide your Date of Birth as mentioned in HRMS and token(if it exists) and confirm your email id.
- If the user has a Security token, he/she will have to choose the appropriate question he/she previously selected and answer of the token he/she recorded.
- Once the question/token is correct and Date of Birth is matched successfully against HRMS, the user would be asked to confirm the Email id to which the new temporary password is to be mailed. Upon confirmation, the password will be mailed to the official mail id. Then the user can change the password as mentioned in the previous section.
- If your Date of Birth or email id does not match with the the info available in HRMS, the user should contact the HR representative to get it corrected in Peoplesoft HRMS application first so that it can be reflected in all applications. The changes in HRMS will be reflected in all other internal applications every one hour.
- Remember not to forward the mail received thus to any one, even to ISG HELP id, since it contains your password.
1.7 **CHANGE SECURITY TOKEN**

A link has been provided on login to enable changing the Security token by the users. This function can be used to create or change Security token.

- Enter your employee id and date of birth.
- Then choose a question and an answer for the chosen question and submit.
- The Security token is created with the combination of question and answer
- Select a question of your choice from the list and give your response to it.
### 1.8 **User Password Management Guidelines Given by Infosec Group**

The policies given in the Information Security Procedure Manual are listed below:

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Policy in IS</th>
<th>IS Policy Addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Password complexity shall be enabled in domain controller.</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>All passwords are valid for a maximum period of one month</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>All user passwords will be of minimum 9-character length. Passwords are not shared and never displayed on the screen in clear text</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>User ids associated with a password are disabled after not more than 6 consecutive failed log in attempts. STG Manager shall monitor such failed login attempts periodically and record the incidents.</td>
<td>Yes / ISG will monitor</td>
</tr>
<tr>
<td>5</td>
<td>Password change shall be forced during the first login.</td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td>Use of alpha numeric passwords with one compulsory special character shall be forced by the application. Passwords for all database instances are unique and maintained in a sealed envelope</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>The above guidelines are followed for SNMP community strings</td>
<td>N/A</td>
</tr>
<tr>
<td>8</td>
<td>The users can change their passwords whenever necessary</td>
<td>Yes</td>
</tr>
<tr>
<td>9</td>
<td>The User passwords/access rights are revoked when an employee leaves the organization. Any resignations / terminations / transfers should be intimated to STG Head / manager by the HR manager for suitable revocation / changes to access rights.</td>
<td>Yes / automated by data update in PeopleSoft HRMS – ISG will monitor this</td>
</tr>
<tr>
<td>10</td>
<td>When passwords are reset and temporary passwords are issued to users, proper identification of the user should be first carried out</td>
<td>Yes</td>
</tr>
<tr>
<td>11</td>
<td>Passwords should never be sent via email or disclosed during telephonic conversations.</td>
<td>Yes</td>
</tr>
<tr>
<td>12</td>
<td>System shall display warning message for users to change the password, from 15th day of last successful password change</td>
<td>Yes</td>
</tr>
</tbody>
</table>