No. FD-FB-109/38/2020-5FB1/ 32747
GOVERNMENT OF PUNJAB
DEPARTMENT OF FINANCE,
(FINANCE BUDGET-I BRANCH)

Dated, Chandigarh the 9 June,2020

To,

    i)   All Special Chief Secretaries, Additional Chief Secretaries,
                Financial Commissioners, Principal Secretaries &
                Administrative Secretaries to Govt. of Punjab
    ii)   All Heads of the Department of the State,
    iii)   All Commissioners of Divisions,
    iv)   All District & Session Judges and Deputy Commissioners of Districts,
    v)   The Registrar, Punjab & Haryana High Court, Chandigarh
    vi)   Secretary, Punjab Vidhan Sabha

Subject: **Instructions for enhancing the security features of Integrated Financial Management System (I.F.M.S.)- Password regarding.**

Madam/Sir,

         I have been directed to convey that the Department of Finance, with an objective to enhance the security of newly rolled out Integrated Financial Management System (IFMS) has decided to lay down the instructions with regard to "Password" as follows:

1. Purpose: The purpose of these Instructions is to lay down the standards for enhancing the security of IFMS through creation of strong passwords, protection of those passwords and the frequency of change of the password along with ensuring the linkage of I.F.M.S. login with i-HRMS code of the employee.

2. Scope: The scope of these instructions include all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on IFMS . Such personnel range from Head of Departments to Drawing and Disbursing Officers (DDOs) on one hand to the designers and developers of individual applications of IFMS on the other hand.

3. Instructions:

    a. For users having accounts for accessing systems/services(HoD/Head of Offices, DDOs etc.):

i. Users shall be responsible for all activity performed with their Username issued by NIC. Users shall not permit others to perform any activity with their Username or perform any activity with Username belonging to any other user.

ii. All User-level Passwords shall be changed periodically, i.e, before the beginning of every quarter of a Financial Year. For e.g: for the quarter July-September, the User shall change the password before generating the Salary bill of June and so on. Users shall not be able to reuse previous three passwords at the time of change of password.

iii. Password shall have a minimum length of 8 characters and comprise of a mix of alphabets in both Upper case and Lower case (A,B,C...; a,b,c,....) numbers (1,2,3.....) and special characters (@,#,$.....).

iv. Passwords shall not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control or in any other location where unauthorized persons might discover or use them.

v. All access codes including User ID Passwords, Network Password etc. shall not be shared with anyone, including Personal assistants or Secretaries. These shall be treated as sensitive and confidential information.

vi. Passwords must not be communicated though email messages or other forms of electronic communication such as on phone to anyone.

vii. Passwords shall not be revealed on questionnaires or security forms.

viii. Passwords should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.

ix. The same password shall not be used for each of the systems/applications to which a user has been granted access e.g. IFMS and e-Office accounts shall have a separate password and so on.

x. The "Remember Password" feature of applications shall not be used.

xi. Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.

xii. The system shall force a change in password on the first time login to systems/services with administrator created passwords.

xiii. If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.

xiv. The password shall be changed immediately if the password is suspected of being disclosed or known to have been disclosed to an unauthorized party.

b. For designers/developers of applications/sites:

i. No password shall be traveling in clear text; the hashed form of the password should be used. To get around the possibility of replay of the hashed password, it shall be used along with a randomization parameter.

ii. The backend database shall store hash of the individual passwords and never passwords in readable form.

iii. Password shall be enforced to be of a minimum length of 8 characters and comprise of a mix of alphabets in both Upper case and Lower case (A,B,C...;a,b,c,....) numbers (1,2,3.....) and special characters (@,#,$.....).

iv. Users shall be required to change their passwords periodically, i.e., before the beginning of every quarter of a Financial Year and a User shall not be able to reuse at least previous 3 passwords.

v. For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.

c. Instructions for constructing a password: All user-level and system-level passwords must conform to the following guidelines:

i. The password shall contain a minimum of eight characters and a maximum of 20 characters.

ii. The password shall not be a word found in a dictionary (English or foreign).

iii. The password shall not be a derivative of the Username, e.g. 123.

iv. The password shall not be a slang, dialect, jargon etc.

v. The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters, etc.

vi. The password shall not be based on computer terms and names, commands, sites, companies, hardware, software.

vii. The password shall not be based on birthdays and other personal information such as addresses and phone numbers.

viii. The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc. or any of the above spelled backwards.

ix. The password shall not be any of the above preceded or followed by a digit (e.g., secret1, 1secret).

x. The password shall be a combination of upper and lower case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as well and special characters (e.g., ! @# $%^&*()_+|~-=\`{}[]:";'<>?,./).

xi. Passwords shall not be such that they combine a set of characters that do not change with a set of characters that predictably change.

4. Responsibilities:

i. All individual users having accounts for accessing systems/services on IFMS and system/network administrators of NIC servers/ network equipment shall ensure the implementation of these instructions.

ii. All designers/developers responsible for IFMS development shall ensure the incorporation of these instructions in the authentication modules, registration modules, password change modules or any other similar modules in their applications.

5. Audit:

i. Personnel authorized for Internal Audit shall periodically review the adequacy of such controls and their compliance by the Users and record the same in their reports specifically.

ii. Personnel authorized as Application Audit shall check respective applications for password complexity and password Instructions incorporation.

6. Timeline of Implementation:

The instructions comes into force with immediate effect, i.e. from the date of issuance and shall remain in force till revoked or modified.

Meticulous compliance of above instructions be ensured.

Yours Faithfully,

(Harwinder Singh)
(Harwinder Singh)

Budget Officer

I.D. No FD-FB-109/38/2020-5FB1/ 32747   Dated, Chandigarh: 9 June,2020

A copy is forwarded to the Chief Secretary to Government of Punjab for kind information.

Budget Officer

To

Chief Secretary to Government of Punjab

I.D. No FD-FB-109/38/2020-5FB1/ 32747 Dated, Chandigarh: 9   June,2020

A copy of the above is forwarded to Secretary Expenditure, Special Secretary Expenditure, Special Secretary Finance and Additional Secretaries Finance for information and necessary action.

Budget Officer

To

1. Secretary Expenditure

2. Special Secretary Expenditure

3. All Special Secretary Finance

4. All Additional Secretaries Finance

I.D. No FD-FB-109/38/2020-5FB1/ 32747   Dated, Chandigarh: 9 June,2020

A copy of the above is forwarded to All Deputy/Under Secretaries Finance for

information and necessary action.

Harhuinder Sur
Budget Officer
R. Kom

To

1. All Deputy Secretaries Finance.

2. Under Secretary Finance.

I.D. No FD-FB-109/38/2020-5FB1/ 32747 Dated, Chandigarh: 9 June,2020

      A copy of the above is forwarded to Superintendent of all Finance Expenditure Branches and Finance Budget Branches for information and necessary action.

Harhuinder Sur
Budget Officer
R. Kom

To

      Superintendent of all Finance Expenditure Branches
      and Finance Budget 2 Branch

      A copy of the above is forwarded to the following for information and necessary action, please:-

1. Director, Treasuries and Accounts, Punjab, Chandigarh;

2. All District Treasury Officers and Treasury Officers, Punjab;

3. Project Manager, IFMS in NIC, Punjab.

Harhuinder Sur
Budget Officer
R. Kom

Endst.no.FD-FB-109/38/2020-5FB1/ 32747 Dated, Chandigarh: 9 June,2020

      A copy of the above is forwarded to the Accountant General (A&E), Punjab and Accountant General (Audit), Punjab, Chandigarh for information and necessary action.

Harhuinder Sur
Budget Officer
R. Kom

Endst.no.FD-FB-109/38/2020-5FB1/ 32747 Dated, Chandigarh: 9 June,2020

Copy to:-

      Private Secretary/ Principal Secretary Finance