REQUEST FOR CREATION OF APPLICATION USER FORM- I

The form to be completed for requesting initial user system access to computer systems of Income-Tax Department or when a logon-ID is to be deleted.

TO BE FILLED BY THE EMPLOYEE

1. Logon Request Type (Please tick the appropriate box) New ☐ Change ☐ Delete ☐

2. Employee Number

3. Place of Posting 4. Building Name

5. Name of employee
Last Name/Surname First Name
Middle Name

6. Date of Birth (DD-MM-YYYY) 7. Designation

8. Assessing Officer Code 9. CCIT/DGIT Region 10. CIT/DIT Charge

11. Full Office Address of Present Place of Posting

Identify the specific system accesses the employee will require to perform his/her work. For access to the computer System and information resources of the Income-Tax Department, a profile is required through which, during initial creation, on-line across is permitted.

	System	Environment			Application Role(s) to be Assigned		Remarks, If any
		D	T	P	Supervisor	System Administrator	
a.	Initial PAN Allotment System						
b.	Assessee Information System						
c.	Tax Accounting System						
d.	TDS Information System						
e.	Assessment Information System						
f.	Individual running Ledger Account System						
g.	Enforcement Information System						
	i) Search and Seizure						
	ii) Survey						
	iii) Tax Evasion Petition						
	iv) CIB System						
h.	Resource Management System						
	i) Financial Resource System						
	ii) Physical Resource System						
	iii) Payroll System						
	iv) Manpower Management System						

D – Development, T – Testing, P – Production, (i.e. work on application systems)

Employee (Signature)

TO BE FILLED BY THE SUPERVISORY OFFICER

Active Date (Date the employee's system access becomes effective through the use of the Logon-ID and password (DD-MM-YYYY)

Termination Date (Date the employee no longer requires system access to perform assigned work, or when terminating employment with the department or office on account of resignation/transfer/retirement/suspension/dismissal etc.) (DD-MM-YYYY)

I have reviewed and agree that the above request is job related and authorize action to be taken

Name of supervisory Officer | Telephone Number | Date sent to System Administrator/Database Administrator (DD-MM-YYYY) | Signature of Supervisory Officer

TO BE FILLED BY SYSTEM ADMINISTRATOR/DATABASE ADMINISTRATOR ONLY

Logon ID/User ID | Initial Password | Date the logon ID/User ID is deleted (DD-MM-YYYY)

Name of the System Administrator/Database Administrator | Telephone Number | Signature of System Administrator/Database Administrator

Copy 1: For System Administrator / Database Administrator

REQUEST FOR CREATION OF APPLICATION USER FORM- II

PROTECTED WHEN COMPLETED.
Note: The Information on this form is collected to provide documentation for administration of automated systems and is protected. The form is stored in Employee Personal record.

TO BE FILLED BY THE SYSTEM ADMINISTRATOR/DATABASE ADMINISTRATOR

1. Employee Number

2. Place of Posting

3. Building Name

4. Name of employee
Last Name/Surname First Name
Middle Name

5. Date of Birth (D D - M M - Y Y Y Y)

6. Designation

7. Assessing Officer Code

8. CCIT/DGIT Region

9. CIT/DIT Charge

10. Full Office Address of Present Place of Posting

Active Date (Date the employee's system access is to become effective through the use of the Logon-ID / User ID and password) (D D - M M - Y Y Y Y)

Termination Date (Date the employee will no longer have system access, or when terminating employment with the department on account of resignation / transfer / retirement / suspension / dismissal etc., or the employee I on earned leave) (D D - M M - Y Y Y Y)

The specific system accesses the employee is permitted to perform his/her work

	System	Environment			Application Role(s) to be Assigned		Remarks, If any
		D	T	P	Supervisor	System Administrator	
a.	Initial PAN Allotment System						
b.	Assessee Information System						
c.	Tax Accounting System						
d.	TDS Information System						
e.	Assessment Information System						
f.	Individual running Ledger Account System						
g.	Enforcement Information System						
	i) Search and Seizure						
	ii) Survey						
	iii) Tax Evasion Petition						
	iv) CIB System						
h.	Resource Management System						
	i) Financial Resource System						
	ii) Physical Resource System						
	iii) Payroll System						
	iv) Manpower Management System						

D – Development, T – Testing, P – Production, (i.e. work on application systems)

Logon ID/User ID

Initial Password

Date the logon ID/User ID is deleted (D D - M M - Y Y Y Y)

Name of the System Administrator/Database Administrator

Telephone Number

Signature of System Administrator/Database Administrator

ACCESS AUTHORIZATION

a. The completion of your normal work duties requires that you have access to "protected" information, files and restricted on-line facilities. In order for you to access these password-protected facilities you will be issued a Logon-ID and an initial password. They are assigned to you and are to be used by you for official use only. You should immediately change your initial password. You should memorize your password, and you are cautioned not to disclose your password to any one.

b. Should you forget your password, or you suspect it has been disclosed you should change it. You should also inform your supervisor immediately so that appropriate action can be taken. Please note that all transactions are recorded and Your access authorization is issued on the basis of the present job you are doing. When you change jobs, your access to the system may also require change. If access to the system entitles you to create any programs, utilities, and/or Job Control Language, you are reminded that whatever you create is the property of the Income-Tax Department.

c. Keep all information confidential and secure according to the classification or designation of that data on the system.

d. Immediately report any known or suspected security incidents to your local security administrator.

TO BE FILLED BY THE EMPLOYEE

This is to acknowledge receipt of my Logon-ID and initial password for access to the system and data resources. I will change my password immediately and restrict my use of the system for job related purposes only. I have read the above Information.

Employee(Signature)

Copy 2: For Employee

FORM-III

IT Security Practices
Responsibilities - Employee

1. This document will help you get to know the Department's Information Technology (IT) security practices. They minimize the risk of compromising sensitive information we store, process or transmit on out IT systems.
2. Please read each section below, and then check the box at the right side of the page to confirm that you have done so. When you have read all sections, please sign, date and return this Document to the Security Administrator.
3. All employees will be granted the system privileges and access to IT systems, Information, and resources of the Income-Tax Department which they require need for their official work related activities only. Accessing and using IT systems of the Income-Tax Department is subject to logging and management review. If employment ends or job duties no longer require it, an employee's system access privileges will be revoked. Remember that all security incidents may be investigated.

Subject	✓
User IDs and Passwords AS an authorised user, I am accountable for all activities performed under my user-ID. Under no circumstances may I share or give my user ID and password to anyone, even a coworker. My password will be a minimum of 8 characters, both alpha and numeric, and random in nature. I will change it at least once a in a month, or immediately if I suspect my password or account have been compromised.	☐
Software and hardware I will use only the approved soft wear supplied by DIT(Systems) on departmental systems	☐
Viruses I am responsible for scanning my workstation (PC) on a regular basis, and for scanning all new or incoming material from other Income-Tax Offices/Government Departments/Agencies or the public before I use it. The anti-virus software approved by the Department is installed on my system.	☐
Using Designated Information **Processing** I am aware that IT systems are protected by approved access	☐
Storage I will keep the magnetic media containing data files which are confidential nature properly under lock and key. I will intimate the location of such files to my Supervisory Officer.	☐
Re-use I will use approved software to overwrite material that is to be re-used. If I am not sure how to do this, or what the appropriate software is, I will contact the IT system Administrator. I will not throw any material in the garbage if I am not sure about its classification. I will give any Material of this nature to the IT Security Administrator.	☐
Destruction I will give any material that can be or needs to be destroyed to the System Administrator or to the Security Administrator, so that it can be disposed according to departmental policies.	☐
Electronic Mail I will use the departmental e-mail systems for official work-related purposes only. My messages will be brief and concise, and I will keep them in the system only for as long as needed to complete work. I will then file them in the departmental Records Management areas, or delete them. I will not transmit confidential Information electronically, unless it is encrypted using departmentally approved algorithms.	☐
Log-off I will ensure that there is no unauthorized access to my workstation by: • activating the screen saver feature with password protection, or by setting my computer system to 'lock workstation' when leave active sessions unattended; and • terminating all active sessions and logging off from the system when I have finished my work	☐
Backups I will save all my documents on the network. I will save documents locally only if the network server is unavailable. Once the server is available. I will transfer these documents back to the sever. I will save documents classified as "confidential" or a higher levewl to atlternative media such as diskette or ZIP disk (see "Sensitive data" below)	☐
Care of equipment I will not move any of my workstation components or install or remove any softwarre of hardware without the concent of thelocal IT section.	☐
Portable computers If I use a portable computer (laptop), it will have departmentally approved encrption software installed and activated. I will properly secure the laptop at all time.	☐
Sensitive data I will encrypt all correspondence sent to clients outside my branch if it is highly sensitive ("Particularly Sensitive" and higher levels). I can transmit any information that is not readily identifiable. I will encrypt any attachments sent via Mail. As an exemple, an unpublished news release should be encrypted – a published news release can be sent without encryption. If I am dealing with documents at the "Extremely Sensitive" level or "Classfied" ("Confidential", "Top Secret") level, I will get a review and sanction from the Security Administrator. High-grade encryuption and stringent security safeguards are required for these documents.	☐
Internet I will not access the Internet through my PC or any other PC of the Income Tax Department which is connected on the Income Tax Network. I will access the Internet only from stqandalone PC which has been duly authorized and for official work reasons. I will not use it to satisfy curiosity or for non-departmental work. I will not sent any sensitive data over the internet unless it is encrypted using departmentally approved encryptionsoftware. Unlawful or unacceptable use is strictly prohibited and can be considered as a cuase for disciplinary action, up to termination of employment and/or criminal prosecution. My Internet password will be different from my TAXNET password.	☐
Modems I will not install or use any Internal or External modem unless the same has been either provided by DIT(Systems) or Dial up / Lines on my PC unless the same has been authorized by DIT(Systems). I will abide by the privisions of I.T. (Information Technology) Act, 2000. I have read and will comply with these security practices.	☐

Name (Please write in Block Letters) Signature

Summary of responsibilities

●**Safeguard Information and equipment**	●**Follow IT security policies**
●**Report incidents to your Supervisory Officer**	●**Turn your computer off when you are away for an extended period to time**
●**Keep you password confidential**	●**Destroy sensitive printouts in the appropriate manner.**

Instructions to fill the Proforma

1. In **Form I**, the column “Environment” the option **[P]** is to be ticked.
2. Officers Officials working in Assessment may use option **(b), (e) & (f).**
3. DDO’s may should use option **(h)** also.
4. The TDS Officers Officials may use option **(d).**
5. The option **(g)** may be used by the Investigation CIB.
6. In **Form II** only items from 1 to 10 may be filled.
7. The option **[a] & [c]** is used by the Computer centre
8. Read the **Form III** carefully and Tick all the options **[√] or [X]** relating to the subject.
9. Forms filled p by Officers Officials should be certified by their immediate Superior Supervisory Officer as required in Form I