



Department of Finance – Division of Revenue and Taxation

User Access Request Form

CNMI Government Computer System

Shaded boxes for EDP service use only

Form RT-UAR

Section A: User Information

1. Requestor's Name: Last Name _____ First Name _____ Middle Name _____			2. Access Unique Login ID (EDP Use Only)	
3. Requestor's Job Title _____		4. Employment Status (Check one) Full-time <input type="checkbox"/> Part-time <input type="checkbox"/> Contractor <input type="checkbox"/> WIA <input type="checkbox"/> Other <input type="checkbox"/> (specify) _____		5. Employee No. _____
6. Contract Expiration Date _____	7. Type of User (see instructions)	8. System Name (Tax System, JD Edwards)	9. Contact no. _____	

10. User Responsibility Agreement Statement

I am responsible for logon/logoff, all actions pertaining to the use of my assigned logon ID, and will not provide my logon ID to another person. I agree that access to computer data or files not authorized to me is prohibited. I understand my logon ID may be suspended indefinitely if I violate security procedures or fail to provide update information for Section A whenever I change job positions. I agree that misuse of the CNMI Government computer system may result in disciplinary action and/or criminal prosecution. I understand that any detected misuse of a computer system will be reported to the proper authorities.

Signature _____

Date _____

11. Manager's Responsibility Agreement Statement

I agree that modifications to existing service agreements will require additional Form UAR requests. I agree that this logon ID will be used for authorized Division of Revenue and Taxation work within the scope of my organization. I also agree that upon termination or transfer of the user, I will advise the Division of Electronic Data Processing (EDP) or the Information Systems Security Officer (ISSO) in writing as to the disposition of the computer files and/or data and logon ID. I will periodically review the use of the assigned logon ID and computer files and/or data.

Manager's Name (please print) _____

Signature _____

Date _____

Telephone No. _____

Section B: Computer Access Requested

12. Describe Support Required

Logon ID (Circle one): New Change

Access for the JD Edwards Subsystem (Payroll, Timekeeping, etc.)

Access for the CNMI Tax System Subsystem (Cashier, BGR, Audit, etc.)

Location Where Access Is Required

Department _____

Division _____

Branch or Section _____ Tel _____

Internet Access (Circle one): Yes No

If your location is outside the CNMI complete the following:

Address 1: _____

Address 2: _____

City _____ State _____ ZIP _____ Tel _____

Section C: Privacy Act Statement

The privacy act is stated for individuals requesting access to the CNMI Government Computer System. The authority in collecting this information is 5 U.S.C. 301. The use of the requesting person's Social Security Number (SSN) is for identification purposes only. Existing users requesting modification or termination of access to the CNMI Government Computer System are not required to provide their SSN.

13. User Acknowledgement (Users requesting system access must read, sign and date prior to submitting this form)

- I have read and understand the Privacy Act Statement and the CNMI Government Computer System Rules of Behavior (see page 2)
- Decisions in personnel matters involving disciplinary action will be based on the assumption that I am familiar with the security requirements presented in these rules and I am aware of my obligation to abide by them.
- I understand that systems require security to protect user and system files from unauthorized access.
- I have completed this form to the best of my abilities.

User Signature

Print Name

Date

Section D: Approvals

14. A. Supervisor

Print Name _____ Approved Denied
Phone Number _____ Date _____ Signature _____

B. Branch or Section Manager

Print Name _____ Approved Denied
Phone Number _____ Date _____ Signature _____

C. Information System Security Office (ISSO) or System Administrator

Print Name _____ Approved Denied
Phone Number _____ Date _____ Signature _____

D. Secretary of Finance

_____ Date _____ Approved Denied
Signature

Section E: Disclosure Officer – Division of Revenue and Taxation

15. Has the privacy training been completed? Yes No

This section is for the Disclosure Officer (DO) use only.

Section F: Division of Electronic Data Processing Use Only

16. Activation Date

17. User ID *(enter here and in box 2)*

18. Has the security training been completed? Yes No

19. Date received

20. Person receiving request *(print name)* Signature

21. Date completed

22. Division Director or designee *(print name)* Signature

23. Comments/Special Instructions

A copy must be provided to the requesting agency after this document is approved and completed.

Rules of Behavior (RoB) – CNMI Government Computer System General User

User ID and Password

The User ID and password being issued to you must not be shared with or given to anyone else. Users who share their User ID or password will be in violation of the Computer Fraud and Abuse Act of 1986. If you forget your password or believe your password has been compromised, contact the Division of Electronic Data Processing immediately. Contact also your local systems administrator if you have one. To have your account reset, contact the EDP division personnel support at 670.664.1407 or 1420 and open a ticket through the Help Desk ticketing system.

Monitoring and Auditing of the CNMI Government Computer System

At any time, the government may monitor and/or audit user activity and/or network traffic. In addition, the government may access your system and disclose information obtained through audits to third parties, including law enforcement authorities. Acceptance of the warning banner prior to logging onto the computer system network is your acknowledgement of the CNMI Computer System monitoring/auditing.

Violations

Violations of information system security guidelines and procedures may lead to disciplinary action up to and including termination of employment.

Manager/Supervisor Responsibilities

All persons in a management role must be aware of and acknowledgeable in information system security practices. Managers are responsible for enforcing these practices within their areas and will be held accountable for ensuring that users are aware of and acknowledge their responsibilities. Management is also responsible for ensuring that all users i.e. Employees, Contract Personnel and Official Visitors attend mandatory computer security training.

Users Responsibilities

User's access to information system resources indicates a level of trust between the User, Management and the Division of Electronic Data Processing. Therefore, Users are held accountable for the following:

- Ensure the ethical use of the Government information resources in accordance with guidelines and procedures.
- Utilize all security measures that are in place to protect the confidentiality, integrity and availability of information and systems.
- Refrain from using information resources for inappropriate activities.
- Adhere to all licenses, copyright laws, contracts, and other restricted or proprietary information.
- Always safeguard User IDs, passwords, smartcards and other means of system security.
- Protect information resources when working remotely by ensuring the latest patches and antivirus software are loaded on your Government Owner Equipment (GOE).
- Limited personal use of the internet is allowed only when you are authorized and it does not interfere with official business nor reflect adversely on the information systems.
- Access only those information systems, network, data, control information, and software that you are authorized to use.
- Know who your Information System Security Officers (ISSOs) are and how to contact them.
- Determine the sensitivity of the information and programs on your computer resources (*e.g. sensitive, confidential, etc.*)
- Avoid the introduction of harmful files/data that may contain spy-ware, viruses, etc. into any computer resource.

If you have any questions on the CNMI Government Computer Systems Security, please contact the Division of Electronic Data Processing at 670.664.1407/1420, your local Information System Security Officer (ISSO) or your systems administrator.

Form Instructions

1. **LAST, FIRST, MIDDLE NAME** - Enter the last name, first name and middle name (*if applicable*) of the person requesting CNMI Government computer system access. If middle name does not exist, enter n/a.
2. **ACCESS UNIQUE LOGIN ID** – Division of Electronic Data Processing use only. Do not use.
3. **REQUESTOR'S JOB TITLE** – Enter current job title (*position*).
4. **EMPLOYMENT STATUS** – Check mark a box or boxes that represent your employment status.
5. **EMPLOYEE NUMBER** - Enter your official six-digit Employee Number issued by the Office of Personnel Management (*OPM*). This is a required entry that is part of your user identification.
6. **CONTRACT EXPIRATION DATE** – If you are a contractor, enter your Contractor Expiration Date. Work Enforcement Agency (WIA) and temporary employees such as intern are considered to be on contractual bases. Please contact the administrative office for this date.
7. **TYPE OF USER** – Enter Government Employee, Contractor or Other. This should correspond with Box no. 4 entry. For example, if you enter “Other”, the corresponding check mark in Box no. 4 should be other.
8. **SYSTEM NAME** – Enter the application system you are requesting to access. Enter CNMI Tax System or JD Edwards Financial System.
9. **CONTACT NUMBER** – Enter the telephone number where you can be reached such as your office telephone number or mobile.
10. **USER RESPONSIBILITY AGREEMENT STATEMENT** – Read and understand the User Responsibility Agreement Statement and the Privacy Act Statement and the Rules of Behavior of the CNMI Government Computer System. Sign and print your name and date. This must be completed prior to submitting this form to your supervisor.
11. **MANAGER'S RESPONSIBILITY AGREEMENT STATEMENT** – The manager must read, sign and date to acknowledge this statement.
12. **DESCRIBE SUPPORT REQUIRED** - Enter the type of access requested for this system. If you are not sure, please contact the Division of Electronic Data Processing (*EDP*) for the appropriate action.
13. **USER ACKNOWLEDGEMENT** – Read the Privacy Act Statement and the Rules of Behavior (RoB), sign and date the user acknowledgement statement. This must be completed prior to submitting this form to your supervisor.
14. **APPROVALS** - Prior to the user submitting the User Access Request form, it must be approved by the following: the user's Supervisor, the Branch or Section Manager, the Information System Security Office (*ISSO*) and the Secretary of Finance, if applicable.
15. **PRIVACY TRAINING COMPLETE** - This section is for the Disclosure Officer (*DO*) use only.
16. **LINE 16 TO 22** - This section is for the Division of Electronic Data Processing office staffs use only.
23. **COMMENTS, SPECIAL INSTRUCTIONS** - Enter any comments or special instructions that are needed for the completion of this request for system access.