

MANUAL FOR COMPUTER MANAGEMENT

Court-Owned Property Policy

A. Purpose and Scope

The purpose is to improve management control and oversight on the use of court-owned computers (including all peripherals, such as fax machines, printers, scanners, or other such equipment). This policy applies to all court personnel (judges, judges' staff, court executives, and all clerical and administrative personnel) who use computers in the performance of their official duties.

B. Authority and Responsibility

The supervising judicial officer is responsible for the management of automated equipment that belongs to the court. The supervising judicial officer will appoint an automation manager.

C. Policy

Court-owned computers may not be used in private residence. The computers are government property and are to be used for official business only. These policies can only be changed or modified with the prior written authorization of [ARD Inc]. These Policies will be reviewed annually, and procedures for monitoring will be determined by representatives of [ARD, Inc].

D. General Use of Computer Resources and Services

1. Computers supplied by [ARD, Inc] are owned by the Kingdom of Nepal. Equipment covered under this manual includes, but is not limited to, the following: host computers, file servers, workstations, standalone computers, monitors, removable drives, USB laptops, software, fax machines, scanners and printers.
2. These resources are provided for official court business to be used to assist the employees in the performance of assigned duties. Since no two employees will use these resources in exactly the same way, each user will have to exercise

individual responsibility and judgment as to appropriate use within the broad guidelines of "official business". Personal use of computers is strictly forbidden. If an employee is in doubt, he will consult with the automation manager, who will consult with the supervising judicial officer.

3. Users are prohibited from storing any material found embarrassing to the court, Ministry of Justice or other entity of the Kingdom. No indecent, profane, obscene, or other unlawful material in any form shall be stored in any court-owned computer.

E. Management Guidelines and Operational Procedures

1. Each court will have a properly trained automation manager.
2. The employee must acknowledge receipt and abide by all of the policies and procedures contained therein and must sign the Computer User Agreement.
3. All software must be installed and used in accordance with the applicable licenses and the software copyrights must not be violated by the user. Software can only be loaded onto the equipment by [ARD, Inc] or their authorized representative.
4. All computers must be periodically scanned for computer viruses. As part of stand automation training, employees will be shown how to utilize software to perform routine protection activities. The [ARD, Inc] representative [or, vendor] will provide the court with periodic updates to the Norton Anti-Virus software for installation on computers. Any detection of a virus will be reported to the automation manager.
5. An audit will be maintained (where property is located physically, what the property is), by the automation manager.
6. The automation manager will be notified of all damaged equipment or equipment which has malfunctioned. No employee shall alter, modify, or repair any equipment or permit other persons to repair or modify the equipment without prior approval of the supervising judicial officer.
7. If equipment is damaged beyond normal "wear and tear" the supervising judicial officer has the authority to cover that loss by garnishment of wages of the employee.

F. Equipment Security

1. The automation staff will provide annual computer security awareness training to ensure that all court personnel are kept informed as technology advances.
2. Employees must refrain from any practice which might jeopardize the courts computer systems, including but not limited to the introduction of viruses, Trojans, or spyware. Employees must be mindful of court sensitive information and records.
3. Employees must take precautions to prevent loss, theft, or damage to court-owned computer property. Employees shall take common sense to prevent theft or damage to computer equipment.
4. Employees should use standard safety precautions when using judiciary computer equipment, including providing a stable and properly adjusted work surface, grounded electrical outlets, adequate electrical capacity, etc. Beverages or smoking is not allowed in the vicinity of computer equipment. Any damage or malfunction must be report immediately to the automation manager.
5. A smoke detector will be installed in the computer room.

G. Physical Security

1. The computer facilities are not marked by any plaque or other markers. The rooms will have steel doors, with bars on the windows. No visitors are left alone in the computer room at any time. The automation staff is responsible for cleaning the computer room. The cleaning or security staff does not have access to the computer room.
2. The computer facility is a secure area; doors will remain locked at all times.
3. A portable fire extinguisher is located in the computer room, and it is the responsibility of the automation manager to ensure that the extinguisher is checked and/or replaced annually.
4. All server systems are protected from power fluctuations with the use of uninterrupter power systems (UPS) located in the computer room. Periodic inspection will be conducted on all UPS.
5. All employees who use computer equipment will have unique passwords. The pass words will be stored in a safe maintained by the supervising judicial officer.

System staff does not have access to the safe, or know it's combination.

6. All system passwords and combinations are changed whenever a member of the automation staff leaves employment.
7. Whenever a court staff employee leaves the courts office or a judge's office, the passwords of the employee are deleted from the system and accounts are disabled.
8. A diary is maintained of all events that affect computers, particularly those events which cause down time and are considered serious.
9. Employees are required to log off their terminals if their terminals are going to be left unattended for long periods of time (i.e. during lunch or meetings).

H. Backup Procedures

It is the responsibility of the automation manager to perform complete (100%) backups each working day on all server systems. If the automation manager is unable to perform these functions, it is their responsibility to delegate the task. If this task is delegated, the automation manager will inform the Chief Judge in writing.

1. Back up tapes will be stored daily in the [Chief Judges] safe.
2. Once a week the automation manager will store the backup tapes off-site.
3. Backup tapes will be replaced on a monthly basis.
4. It is the responsibility of the automation manager to clean the tape drive regularly and to annually check the hard drives on all PC for unauthorized material.
5. The backup procedures must be posted in writing on the wall of the computer room.

I. Software

1. No software of any kind may be installed unless authorized by the representative from [ARD, Inc] and must be installed by the automation manager. Software that is not installed in accordance with these guidelines will be removed.
2. Copyrighted software must not be reproduced, except as permitted by the terms and conditions of the contract under which it was purchased. All applicable laws must be obeyed.

3. Use of pirated software is prohibited.

J. Equipment Protection

1. All external drives [A and C] will be deactivated to prevent introduction of virus or other items prior to installation of the equipment in the court.
2. Keep food, drinks and electrical appliances away from all computer equipment.
3. Label diskettes and CD's. Left out and unlabeled may be picked up and used by others.
4. Do not bring or download unauthorized or personal software to work.
5. Unauthorized reproduction or copyrighted software or documentation is against the law.

K. Inventory

The automation manager is responsible for maintaining an inventory of all computer hardware and software. The [Chief Judge] is the custodian of all computer equipment. The hardware inventory must include a description of each piece of equipment, the acquisition date, location of the item and condition of the item. The software inventory must include a description of each type of software, the acquisition date, location of the software. No computer equipment may be disposed of with out prior written approval of the authorized representative of [ARD, Inc.

1. An inventory must be performed by the end of [March] of each year.
2. Each piece of hardware must be marked with an identification tag that is easy to read.

Computer User Agreement

As a user of computer resources and services of the [Special Court of the Kingdom of Nepal],

1. I understand that failure to sign this memorandum of understanding will result in denial of access to computer equipment.
2. I understand the policies outlined in this agreement and I agree to abide by the agreements.
3. I will not attempt to gain unauthorized access to computers, networks, or telecommunications nor attempt to view or use electronic files for which I am not specifically authorized.
4. I promise not to take any actions which will jeopardize the security of the judiciary's automated information systems after my departure from employment with the court.
5. I acknowledge my responsibility not to download or install executable software from any source onto the judiciary computer equipment without prior authorization.
6. I understand that I am responsible for the proper use, care and responsible protection from damage or loss of equipment that I use.
7. I understand that I am responsible for maintaining the current level of security available on my work station.
8. I understand is strictly forbidden to use computer equipment for personal use, or to remove it from the building without prior written authority.
9. I acknowledge my responsibility to confirm to the requirements and conditions set forth in this agreement, and I will abide by all applicable policies.

Signature

Date