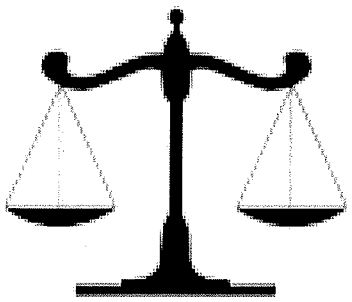
Judicial Service of Ghana



INFORMATION AND COMMUNICATION TECHNOLOGY POLICY AND PROCEDURES

July 2008

TABLE OF CONTENT

Judicial Service

INFORMATION TECHNOLOGY POLICY AND PROCEDURES

The Judicial Service (JS) maintains a collection of computer hardware and software (the Judicial Service Computer System) for the use in providing speedy justice delivery. It is intended to be used by Judges, Cashiers, Process Clerks, System Managers and Court Managers and any other staff whose work demands the use of such equipment in the delivery of justice.

The hardware is arranged as stand alone PCs in some instances and others are connected in a network. This policy guideline is intended for all users.

The establishment of a network system allows for a multi-user environment and as such requires responsible behaviour on the part of all users. This document lays out the responsibilities of users in having access to the Judicial Service computer System. All users who cannot fulfil their responsibilities, as users will be appropriately sanctioned.

1.0 PURPOSE

The purpose of this document is to ensure an information technology infrastructure that promotes the basic mission of the Judicial Service of providing an improved, speedy justice delivery. In particular this document aims of promoting these goals:

- To ensure the integrity, reliability, availability, security and performance of IT resources.
- To ensure that IT resources are used for their intended purposes.

2.0 SCOPE

This policy applies to all users of IT resources, and to the use of all IT resources. These include systems, networks, and individual usage under the management of Judicial Service.

3.0 RIGHTS AND RESPONSIBILITIES

Computers and networks can provide access to resources in the Judicial Service as well as the ability to communicate with others worldwide. Such open access is a privilege, and requires that the individual users or those who have access to the Judicial Service ICT facilities act responsibly. Users must respect the rights of other users, respect the integrity of the computer systems and other related physical resources, and observe all relevant laws, rules, regulations and contractual obligations.

Every staff whose duties require the use of computer will be given an access account and password on the Judicial Service system by the authorised body assigned to do that.

4.0 GENERAL RESPONSIBILITIES

In the performance of individual duties and functions, staff must adhere to the highest principle of ethical conduct on to the public, clients, co-workers and employers.

The Judicial Service computer system as a shared resource, it is important that the system functions as smoothly as possible with minimal disruption and fair access to all. This means that each user has the following responsibilities while using the system:

i. **Do not interfere with the work of other users**. This means that you must not send unsolicited messages to other users, terminal screens, or engage in other activities, which prevent them from accomplishing their assigned work.

ii. **You may not attempt to obtain the passwords of other users or alter their files in anyway even if they should leave their account accessible by failing to log out or alter their protections**. Any user found in the possession of other user password, copying another file without permission would be sanctioned.

iii. **Do not allow others to use your password/Account**. Report unauthorized access. Your password is issued solely for your use. Under no circumstance should ANY other person use your password. Use of another user's account or loaning account privileges to others is prohibited and will result in loss of your account. You are required to notify the Director, ICT immediately of any unauthorised access to your account (e.g. if you find your files missing or changed, or if you find someone else logged into your account from another terminal.) It is essential that such access be detected and the responsible person located to ensure that the system security is not compromised in any way, which may result in the loss of everyone's files or interference with normal operation of the system.

iv. If you do find that someone has used your account, change your password immediately and then report your finding to the Director

v. **Guard your password carefully and change it frequently**. Passwords guessed or determined by watching users log in are the most common means by which accounts are penetrated. Users can help to prevent this by the following measures:

- Never give out your password to anyone else. NOTE: this includes the LAN Administrator.

- Do not type your password whiles someone else is watching you.

- Change your password frequently. The LAN Administrator
- will assist you on request.

- Never use a password based on personal reference data e.g. names of family members birth days, social security number etc

- Do not use a password, which would appear in a dictionary.

vi. **Do not make copies of any software, judicial service information or data for use on other computers**. Unless given explicit permission you may NOT copy any file, data or software from JS computer system to be used at home or on any other computer. Remember any user who copies licensed software is liable to legal action by the software manufacturers. Accordingly, the use of illegal or unauthorised software on the Judicial Service Computer System is prohibited.

vii. **Do not use your account or computer for private or commercial endeavours**. The Judicial service facilities, including software, hardware and network are intended for the exclusive use of the Judicial Service. Any other use of the facility is prohibited.

viii. **Always cooperate with requests from the LAN Administrator for information about your computing activities.** At times, the LAN Administrator may find it necessary to ask you why you are consuming so much resource, or some information about your use of the system. If asked, please assist in whatever way you can. There only reasons for asking you these questions are to enable them pursue system improvements.

ix. **Report any security flaws immediately.** All multi-user systems have security flaws. You do not exploit such flaws in any way. Should you detect such flaw notify the LAN Administrator immediately. Help the system management to track down bugs, by contacting them and volunteer your services and information.

5.0 MISUSE OF COMPUTING RESOURCES AND PRIVILEDGES

Misuse of computing resources and privileges, as determined by the LAN Administrator includes, but not restricted to the following:

- Attempting to modify or remove computer equipment, software, and peripheral without proper authorization.

- Accessing computers, computer software, computer data or information, or network without proper authorization, regardless of whether the computer, software, data, information, is owned by the Judicial Service.

- Sending fraudulent computer mail or breaking into another user's e-mail box.

- Violating any software license agreement or copyright or redistributing copyrighted computer software, data, or reports without the proper, recorded authorization.

- Taking advantage of another user's naiveté or negligence to gain access to any computer account, file, data, software or file other than your own.

- Encroaching on others' use of the Judicial Service computers (modifying system facilities, operating systems, disk partitions, attempting to crash the computer, damaging or vandalizing the equipment, software, or computer files.

- Disclosing or removing proprietary information, software, printed output or magnetic media without explicit permission of the owner.

- Any other conduct or practices that will discredit the Judicial Service.

6.0 LAN Administrator's RESPONSIBILITIES

The use of the Judicial Service resources by the LAN Administrator's is governed by the same guidelines as any other user's computing activity. However, a LAN Administrator's has additional responsibilities to the users of the network, site, system that he /she administers.

- A LAN Administrator ensures that all users of the system have access to the appropriate software and hardware required to perform the required duties of the user.
- A LAN Administrator is responsible for the security of the system.

- A LAN Administrator must make sure that all hardware, and software agreements are faithfully executed.

- A LAN Administrator must take reasonable precaution against corruption of data or software or damage to hardware or facilities.

- A LAN Administrator must treat information about and information stored by the system's users as confidential.

- In the case where a LAN Administrator has reasonable cause to believe that the system response, integrity, or security is threatened, he/she is authorized to access files and information necessary to find and resolve the situation

7.0 SECURITY OF THE SYSTEM.

7.1 Operational Backup and Restore

The Database Administrator will:

- Limit the consequences of the loss or the unauthorized or erroneous modification of information (including damage from malicious programming such as viruses):
- Make backup copies of information with sufficient frequency to balance potential effort required to recreate the information.
- Protect backup copies of the information to the same level as the original information; store offsite as appropriate for software recovery purposes consistent with disaster recovery plans. Management will determine the offsite.
- Recognize the difference between operational backups, necessary to restore system functionality in case of hardware, operating software, or application software failure, and copies of information archived to meet records retention requirements. Operational backups should be erased, overwritten, or otherwise made unreadable as soon as the requirement for the backup is exceeded.

Protect information during storage or transmission.

Securing the system includes:

- Assessing the quality and reliability of storage media to ensure records retention requirements are met.
- Protecting removable media (diskettes, disks and hard drives, and hardcopy, etc.) containing critical information in operations environments from unauthorized disclosure through physical removal.
- Usage of a storage system that avoids descriptive external labels. (i.e. labels that invite unwanted interest like PRIVATE or PROPRIETARY)
- When exchanging information (media) with external parties, establishing appropriate controls to prevent unauthorized use or disclosure of the information.

To minimize the extent or duration that information is potentially exposed to unauthorized disclosure:

- Destroy all primary and backup copies that are no longer needed. Comply with organizational records retention guides as directed by management and, where applicable, with corporate guidelines for disposal of classified information.
- Use appropriate destruction methods for various computer information storage media such as:

Tapes: physical destruction, writing over, or demagnetising

7.2 Standards and General Practices.... Disaster Recovery

i. Design procedures to prepare, store, and periodically test the integrity of off-site backup copies of all information necessary to restore the system to normal operation, including:
   - Data
   - Operational procedures
   - Software documentation
   - Systems software
   - Contingency plan documentation

ii. Design procedures to recover backup information if the operational copies of the information are lost or destroyed.

iii. Do not use off-site backup copies of information except to make a further copy. After making the further copy, return the original backup copies immediately to off-site storage.

iv. Establish backup data storage facilities at a separate site that is unlikely to be affected by the same disaster events as the prime site. The backup site must provide a secure environment for ensuring the integrity, confidentiality and availability of backup information.

7.3 Operational Backup and Restore - Minimum Guidelines

Various forms of information backup approaches are used at sites based on platform, service, business requirement, and application risk. The following are some minimum guidelines for establishing/upgrading local procedures.

Typically backups have three purposes.

- To allow restores when a file gets corrupted or in the event of a disk failure.
- To allow recovery in the event of a disaster.
- To address record retention requirements.

Each has varying backup, storage and retention requirements and must conform to the requirements of the Judicial Service.

7.4 Schedule of Backups

Backups must be done on a daily basis in various forms of Incremental, Differential and Full backups. Differential backups will be carried on off-hours (closing time) of weekdays. But full backups will be carried on Fridays, at off hours, the last working day of the week. A full backup should be done at least once a week. A schedule should be developed and kept in the procedure manual.

7.5 Verification

A designated staff member should verify that all backups completed successfully. If a backup fails, the appropriate server contact should be notified as soon as possible so the backup can be processed manually.

8.0 TAPES AND DATA RETENTION

Tapes and data should be retained based on specific system, application or service requirements. These requirements should be formalized and documented.

8.1 Labelling/Inventory

Records should be kept of what backups have been made, where the storage medium are stored and on what medium to find versions of a file. You may keep this inventory online. A hardcopy of this should be made from time to time. The medium should be clearly labelled.

The number of times a medium is reused should also be kept so it can be correctly disposed of.

8.2 Restores and Testing of Tape/Disk Backups

The activity to restore the data must be logged by the system. Operations management must make periodic checks (at least spot checks) to ensure that the proper approvals are being obtained and procedures to restore are being followed. Evidence of these reviews has to be kept.

When storage medium are recalled from the offsite storage facility, care must be taken that only those with proper authority receive the back-up media

Testing of restore procedures should take place at least once a year. Most sites have the opportunity to test their backups via normal restore requests. Where sites do not have frequent restore activity, they should conduct a random sampling on an annual basis. Sites can also test their restore capability via their annual disaster recovery plan test. In whatever form, the successful test should be documented.

Some backup/restore tools or commands have an option to perform a "logical reload" at the end of a backup execution. This option simulates a restoration and should be used when available. Success of this feature needs to be checked daily.

9.0 PC INVENTORY

9.1SYSTEM SUPPORT SUPERVISOR responsibility

System Support Supervisor is responsible for maintaining detailed records of computer equipment (e.g. PC, printers) including characteristics, location and placement into service and to provide such information to the Assets Management Department.

9.2SYSTEM SUPPORT SUPERVISOR PC inventory Database

By default, a workstation will be considered as a single asset (its control unit being the item of reference). System Support Supervisor records will include:

Equipment type
Serial number (Control Unit serial number for a PC)
Location (including storage room)
Date of installation
User name (considered as PC custodian)

Optional:
Local identifier (usually called Workstation or Material Number)

Equipment will be recorded when receipt by System Support Supervisor.

Information will be recorded in a file/database (e.g. Excel sheet or Access DB) or a dedicated package. Access will be restricted to authorized individual only.

9.3 Physical PC Inventory

System Support Officer will complete physical inventory as per the Company or local affiliate requirements. However, random physical checks will be conducted to ensure, at year-end , a coverage of:

100% of equipment in storage room
100% of laptops allocated
100% of installed desktops

Conclusion of physical checks will be timely reconciled with the database records. System Support Supervisor is not, however, responsible for maintaining equipments related depreciation, depletion or amortization.

9.4 Physical protection

System Support Supervisor will regularly remind PC's custodian (end-users community) of their responsibilities about the physical protection of their computing materials.

9.5Disposal and Transfer

Equipment disposal or transfer of PC equipments will be conducted at least 1 / year.

All equipments to be sold, retired or transfered will be listed. For each material, this document will typically mention :

Justification for disposal or transfer
Current location
Residual value
Action plan (e.g. destruction, donation to employee or charity, sell...)

The list will be reviewed and signed by the Management in collaboration with the Director, ICT . This list will be provided to the accounting Dept).

Before being disposed, all information and files residing on PC disk or any other media will be removed. Typically, hard disk will be formatted.

10.0 REPORTING FAULTS, MAINTENANCE OF PCS & EQUIPMENT

A logbook must be kept by the Help Desk Coodinator to log in all faults and when such faults were rectified. A table as shown below must be kept. Users of any equipment must report faults by completing the fault form and submit it to officer responsible or to the system coordinator. The maintenance firm will then be contacted for the problem to be addressed.

All faults must be reported to the Help Desk Coordinator .
Repairs on any of the Judicial Service equipment will be done on the instructions of the Coordinator.
The System Support Supervisor must be informed of any major repairs that need to be undertaken.

Companies assigned to undertake maintenance and repairs on any property of Judicial Service must strictly adhere to the confidentiality code of the service.
Sensitive information must be backed up and subsequently erased from equipment by user before an equipment is sent to a work shop.

10.1 Removal of equipment from the premises of Judicial Service

Any piece of equipment that needs repair outside the premises of the Judicial Service must be documented and authorised by the System Service Supervisor (SSS). Under no circumstance should equipment be moved out without the express authorisation of the SSS .

10.2 User fault reporting form

Date	Type of equipment	Problem observed	Location Of equipment	User Reporting Fault	

10.3 Fault reporting form to Maintenance

Date	
Serial No of equipment	
Location of equipment	
Name of repair person	
Type of Equipment	
Fault observed	
User's Name	
Signature of repair person	
Remarks on repair	
Signature of System Support Supervisorr	

10.4 Problem log sheet

Record no.	Reported Date	Brief Description of Problem	Problem Assigned to:	Resolution Planned Date	Completion Date
0001					
0002					
0003					
0004					
0005					
0006					
0007					
0008					
0009					
0010					
0011					
0012					
0013					
0014					
0015					
0016					
0017					
0018					
0019					
0020					

11.0 USER ID AND PASSWORD MANAGEMENT

11.1 Creating, Modifying & Deleting User IDs

a. Requesting a new ID

When a new user ID is required, the user should complete a 'User ID Request Form' (see attachment). The form should be approved by the appropriate signatories who as a minimum include the requestor's supervisor and application owner. The form should then be given to a LAN Administrator for implementation.

b. Setting up a new ID

On receiving the form, the LAN Administrator creates the new user ID on the required system(s). Where technically possible, the ID should be set up to force the password to be changed at first logon.

Once the ID has been set up, the access Manager signs and dates the User ID Request Form to confirm that access has been granted. This form is then stored in a folder.

c. Informing the user of

the new ID details

It is preferable that the new user ID and password details be supplied in person by the access Manager to the user.

Where this is not possible, supplying the ID and password via internal mail is preferred.

d. Modifying an ID

If an ID needs modifying (e.g., access to new shares or a change in privileges), then either a new form with the required authorising signatures should be completed outlining the necessary changes.

The modifications to the user's ID and accesses, once implemented can be communicated directly to the user.

A copy of the modification form, or an electronic copy of the supervisor's e-mail is stored.

e. Deleting an ID

When an ID needs to be deleted, the supervisor of the ID owner should inform LAN Administrator requesting the deletion. A copy of the supervisor's request should be kept.

An ID can be disabled after 90 days without use and deleted after a further 210 (making 300 days in total) **without** consultation with the ID owner or their supervisor. These obsolete IDs will typically be identified during the annual access review.

f. Retention

All forms and e-mails requesting ID creations, modifications and deletions are stored by the LAN Administrator (on paper or electronically) for at least two years.

g. Log Reviews

Access Manager ID creation, modification and deletion activities are monitored via independent log reviews.

Review by an independent person

An independent individual reviews the logs by checking all the LAN Administrator activity. A sample of the IDs created, modified and deleted will be checked against the requests, which have been received by the access Manager.

The supervisor will randomly perform additional monthly reviews.

12.0 LAPTOP CARE AND USAGE POLICY

The Laptop/Notebook computer that has been assigned to individuals should be considered as a tool enabling them to function effectively and efficiently in their job responsibilities. This tool should be regarded as a fragile device that must be handled with the maximum care**. Please treat the computers with the utmost diligence.**

In order to derive maximum benefits from this investment the following **CARE POLICY must be strictly observed.**

i. **OWNERSHIP:** the Judicial Service owns The Laptop allocated to– **Courts as part of the automation process** and therefore data of personal nature may not be stored on the Laptop. Laptops may be retrieved from judges leaving the Services of such courts and reassigned to judges servicing the courts earmarked for automation. This Laptop is to be used solely by Judges. Any other person, including another judge, without the prior written agreement of the Chief Justice, is not permitted to use it.

ii. **Food, Drinks and Smoke:** Please do not eat, drink nor smoke over your computer. Accidents do happen and when they do the consequences can be disastrous. Besides, food particles attract vermin and other pests.

iii. **H_2O**:Laptops are not waterproof. Keep it out of rain and away from bodies of water.

iv. **Cleaning**: When the Laptop screen is to be cleaned, use a soft, lint-free, ***DRY*** cloth and wipe gently with the computer set to off. Do not blow the keyboard with your mouth, you may use canned air

v. **Floppy Disks**: Do not store original working copies of documents on floppies. Use floppies only for backup purposes. Take care that floppy disks are in good condition before putting them into the computer. Faulty or damaged disk will ruin your floppy disk drives.

vi. **Battery Care**: When starting to use your battery for the first time follow the instructions that came with the equipment. The battery should be completely drained before being recharged.

vii. **Transport**: Always carry the Laptop in its proper carry case and never leave it in a car for a long time. Extreme temperatures can damage the motherboard, bake the diskettes, and roast the interior of the computer. Please be careful when removing and storing cables (they break VERY easily and are expensive to replace.) if the laptop is bumped or jolted while being transported, the hard drive or the Laptop may be damaged. Carefully detach and unplug all the components of the Laptop. Take time to neatly pack

- Phones
- Any part of the installation used by other staff of the service.

16.0 Data information exchanges.

i. Do not slot in any storage medium whose origin you do not know.
ii. Use storage medium sanitised and supplied by the appropriate Judicial Service authority. All Judicial Service storage medium must be properly sanitised and labelled by the appropriate authority.
iii. No copy of Judicial Service information should be given out either on electronic media or hard copy without an expressed authorisation from the Judiciary Secretary.

17.0 CLEANLINESS OF YOUR EQUIPMENT AND OPERATING ENVIRONMENT

Users are responsible for the cleanliness of their Workstation; monitor, keyboard and mouse.
Printers and other peripherals. Network outlets, cabling and other components and Phones.

18.0 WHAT HAPPENS IF YOU DON'T ACT RESPONSIBLY?

The Judicial Service considers any breach of your responsibilities to be a serious offence and reserves the right to apply any appropriate sanctions against you.

19.0 SERVICE PROVIDER RESPONSIBILITIES

All service providers are expected to offer service in the most efficient, reliable, and secure manner while dealing with the Judicial Service. At certain times, the process of carrying out these responsibilities may require certain actions or interventions by service provider's staff. In such circumstances, service providers are bound by the policies governing their actions. At all other times, no staff has special rights above and beyond those of other users; they are required to follow the same policies and conditions of use that all users must follow. Every effort shall be made to ensure that persons in position of trust do not misuse the computing resources or data, or take advantage of their positions to access information not required in the performance of their duties.

When service providers are aware of violations, either through the normal course of duty or by a complaint, it is their responsibility to initiate an investigation and at the same time, to forestall an immediate threat to security of a system or its users, service providers may suspend access of the users involved in the violation while the incident is being investigated. They may take other actions to preserve the state of files and other information relevant to the investigation.

20.0 Help Desk

A help desk mounted at the Judicial Services head office in Accra to respond to users requests for help. As much as possible the help desk will provide help instructions on the telephone for the users to follow. Help will be provided for job related problems. As much as possible malfunctions and equipment break down must be reported to the help desk as soon as they occur. Call 021 – 662364 for any assistance.

21.0 VIRUS ATTACKS

Viruses pose a threat to any one who uses a computer. The service will at all times provide anti-virus software and constantly upgrade it. Nevertheless, prevention of virus infestation is the duty of all users. User are therefore urged to refrain from using storage medium whose origin are unknown/ from sources from other machines whether within the service or without.

22.0 ENHANCING THE SECURITY OF THE SYSTEM

To protect information on the system and from getting into the wrong hands, only the Registrar or someone he has delegated can print information from the system. After the completion of a case, information on that case will be removed from the user domain. Read Only permission to access such information will be granted only to the chief Registrar or head of the registry.

It is emphasised that no user shall make unauthorised copies of the Judicial Service stored information. The public who are interested in any information should contact the Registrar who will determine their needs and respond appropriately to it. For the avoidance of doubt no proceedings or information on any PC should be released without the usual application and authority from the Registrar and the payment of the appropriate fees.

23.0 INFORMATION FILING PROCEDURES ON THE SYSTEM

All files and documents should be stored according to created and labelled folders. Folders are created according to Judges handling the case. In capturing information on a particular case, ensure that you are very much aware about the judge handling the case.

Within this folder for a judge, other folders are created according to cases labelled as such. Each case must belong to a folder, and a case folder must belong to a Judge folder. All files must be stored in their respective folders. There should never be an instance where file do not belong to an existing folder.

The data entry clerks/secretaries will be held responsible for files without folders. The Database Administrator will take daily backups of what has been completed for the day into a folder that only authorised users can access.

When a ruling has been given in a case, the complete folder will be assigned to folders for completed case. Two backups on CD ROM are created for all completed cases. A secured off site location may be identified as a place to keep a copy of the CD ROM. The second copy of the CD-ROM may be kept with the supervising Judge.

Off site storage facilities shall be:

- Located for the first backup and should be far enough away so that its not impacted by same disaster
- Provided with physical controls, such as security, authorized access, environmental (heat, humidity, water, and fire protection).
- Located that Retrieving the backup should be possible on demand.

All backup file /CDs should be well labelled to identify their contents. A list of those authorized to retrieve them must be compiled and given to the appropriate authority.

24.0 SEMI –AUTOMATED COURTS

The supervisors of the data entry clerks will create folders just as specified above. The supervisor will ensure the data integrity and security of information on each machine. In order to do that he must take regular backups of the jobs done for the day. He may log in as a different user with a password only known to himself. In order to eliminate any unexpected situation, a double back up should be undertaken as a safeguard.

25.0 DOCUMENT UPDATE

This document will be updated from time to time to reflect the objectives and policy direction of the Judicial Service.