

LAKE BASIN DEVELOPMENT



AUTHORITY



INFORMATION & COMMUNICATION TECHNOLOGY (ICT) POLICY

P.O BOX 1516
KISUMU
EMAIL: info@lbda.co.ke
WEBSITE: www.lbda.co.ke

TEL. 254-057-2027227
FAX: 254-057-2027370

March 2009

	<i>Page</i>
1. Introduction	2
1.1 Preamble	2
1.2 Objectives	2
2 Definitions	2
3 Policy Statement	3
3.1 Accessibility	3
3.2 Confidentiality of Information	3
3.3 Acquisition of hardware and Software	3
3.4 Pornography/Hatred	3
3.5 Physical security	3
3.6 Data Security	3
3.7 User Privacy	3
3.8 Server Security	3
3.9 Fair Warning	3
3.10 Copyright	4
3.11 Network Expansion and Resource Utilization	4
3.12 Purpose of use	4
3.13 Viruses	4
3.14 Internet	4
3.15 Intranet	4
4 Rules and Procedures	5
4.1 Accessibility	5
4.2 Confidentiality of Information	6
4.3 Acquisition of Hardware and Software	7
4.4 Pornography/Hatred	8
4.5 Physical Security	8
4.6 Data Security	9
4.7 User Privacy	10
4.7.1 Privacy – exceptions	11
4.8 Server Security	11
4.8.1 General	11
4.8.2 Access Control	13
4.8.3 Logging	13
4.8.4 Disk Use	13
4.8.5 Backup	14
4.8.6 Communications	14
4.8.7 Specific Password Guidelines	15
4.9 Fair Warning	16
4.10 Copyright	16
4.11 Network Expansion and Resource Utilization	17
4.12 Purpose of Use	17
4.13 Viruses/worms	18
5 Non-Compliance	19
6 Due Process	19
7 Specific Proscriptions	20

1. INTRODUCTION

1.1 Preamble

In order to fulfill its mission, the Lake Basin Development Authority (LBDA) is committed to providing a secure, yet open network that provides the integrity and confidentiality of information while maintaining its accessibility. The company considers Information & Communication Technology (ICT) as an agent of transformation of every facet of corporate life, which will bring about knowledge- based workforce.

This document is meant to serve as a guideline on all ICT related matters within the organization. It shall address user behaviour towards the investment, hardware acquisition, service, and maintenance after warrant period including repair, software procurement and guard against illegal usage (piracy) together with maintenance contracts.

1.2 Objectives

- 1.21 To standardize computer security
- 1.22 To promote confidentiality, integrity and availability of corporate information.
- 1.23 To harmonize and coordinate network expansion initiatives
- 1.24 Maximize use of ICT resources to ensure return on investment.

2. DEFINITIONS

- 2.1 Computing Resources - include, but are not limited to, computer hardware, software, communications equipment and supplies.
- 2.2 Users: - include the following groups:
 - 2.21 Current operations, administration and support staff
 - 2.22 Others authorized by Information & Communication Technology Systems (ICTS)
- 2.3 Workstation - Any device attached to the Company network for the purpose of accessing, transmitting or storing data.
- 2.4 Software - means the operating systems, packages purchased off the shelf and applications, either general or customized.
- 2.5 Server - means any of administrative, operations, mail, web or file servers.

3. POLICY STATEMENTS

3.1 Accessibility

Only those designated and approved users will have access to the computer resources. All resources are intended for shared use within the company community and are to be used in a reasonable and responsible manner.

3.2 Confidentiality of Information

Each user is accountable for ensuring the confidentiality and integrity of information accessed, maintained or disseminated consistent with legislated policies and Authority's policies, procedures, terms and conditions.

3.3 Acquisition of Hardware and/or Software

All ICT systems purchases (i.e. computer hardware, computer software) must be coordinated with the Information & Communication Technology Systems (ICTS) and must be identified as a priority within the computer plans of the area.

3.4 Pornography/Hatred

Company resources are not to be used to access, create, transmit, store or copy information that is obscene, threatening or harassing.

3.5 Physical Security

All computing equipment must have reasonable physical security in place (i.e. reasonable measures to prevent theft and vandalism).

3.6 Data Security

No person or persons shall, by any willful or deliberate act, jeopardize the integrity of the computing equipment, its systems programs or other stored information.

3.7 User Privacy

All users must respect each user's right to privacy.

3.8 Server Security

All server machines in the network will be administered by ICT Department Head and authorized staff using the best practices, and will be located in a physically secure place in a stable environment with backup servers and standby power supply.

3.9 Fair Warning

All users of computing resources have the right to fair warning of the existence of policies and procedure and share in a responsibility for compliance.

3.10 Copyright

Any copying of software, except as expressly stated in the licensing contract of the software, is prohibited. The Company will assist any software supplier with just cause, to prosecute any individual violating the copyright laws.

3.11 Network Expansion and Resource Utilization

All network expansions and resource allocation shall be coordinated by ICT Departmental Head.

3.12 Purpose of Use

The Authority's computer equipment is only for company related activities.

3.13 Viruses/Spy ware/Worm codes

Risks to the company systems/ programs are to be eradicated by deploying appropriate protective systems, devices, coupled with application of best practices.

3.14 Internet

Access to the Internet and its services is provided for the benefit of network users especially for purposes of communicating and research work. End users are expected to act responsibly in their usage of the Internet.

3.15 Intranet

The Company network has been established to provide access to users in all the site to shared internal resources, services and corporate information.

4. RULES AND PROCEDURES

This section is prepared to provide the company with a set of rules and procedures.

4.1 Accessibility

Rationale:

Computing resources are intended for shared use by authorized users.

Procedures:

- a) Authorized persons will have access to the computer resources and may be asked at any time to produce valid identification.
- b) All employees of the company are entitled to access to the Organization's ICT Systems, subject to the approval of the immediate supervisor. In order to complete this process the supervisor may send a mail message to ICTS with the required information or the User Account Modification Form may be completed.
- c) Hours that the computer resources are available must be communicated.
- d) Routine review of the current validity of the following information is required: the level of quotas, privileges and resource allocations; software accessibility.
- e) Where a software borrowing process exists, then this process needs to be documented and communicated to those people borrowing the software.
- f) Users should be aware of and seek assistance from the appropriate resource (i.e. Supervisors, reference manual, Information Technology Systems (ITS) staff, etc.) in the event of problems.
- g) Users are expected to adhere to the requests of LBDA's employed computer technicians or experts.
- h) All hardware and software problems should be immediately reported to the appropriate staff member of ICTS for corrective measures

4.2 Confidentiality of Information

Rationale:

All data must conform to company policy on release of information.

Procedures:

- a) Users must be present when printing confidential material. No document of a confidential nature should be printed or left in an area accessible by other users.
- b) Disks should be properly labeled and stored in a manner, which protects them from unauthorized access.
- c) Confidential information must be destroyed in a manner, which prevents it from being reviewed by others. This may involve destroying reports in the user's own department and not using the garbage cans in the printer areas. Use of a shredder is highly recommended.
- d) Computer resources are to be situated so that the privacy and confidentiality of information accessed is maintained.
- e) It is necessary to log out of the computer before leaving your station unattended.
- f) It is the responsibility of each employee to ensure that confidential or "protected" information is secured and this information is not provided to other people.
- g) All user system data handled by Information & Communication Technology Systems (ICTS) staff must be considered as confidential and not to be discussed with anyone unless the discussion is pertinent to the work of the project team. In the situation of non-compliance, disciplinary action may be taken.
- h) Since all employees of the Company can be issued with an account, there is no reason to provide your username and password to anyone. Should this type of a breach of security occur, or be perceived to occur, the user account will be deactivated immediately until such time as the computer integrity is re-established.
- i) Every user authorized to access computing resources shall be expected to treat as privileged, any information not provided or generated by the user which may become available to the user through computer resources; users shall not copy, modify, disseminate or use any part of it without permission of the appropriate person or body.
- j) Technical staff assigned to ensure the proper functioning and security of Authority's electronic information resources and services are not permitted to search the contents of electronic communications or related

transactional information except as provided for in this Policy. For example, any scanning of network traffic to detect intrusive activities must follow established LBDA's guidelines or organizational procedures to ensure compliance with laws and policies protecting the privacy of information.

- k) Standard reports e.g. pay slips should be dispatched under signature to the authorized persons.
- l) Ad hoc reports, screen formats, print-outs in total or partial should not be dispatched to unauthorized persons and especially third parties.
- m) Users must not attempt unauthorized access of computer installations outside of the company using the Company's computing resources

4.3 Acquisition of Hardware and/or Software

Rationale:

To coordinate all Information & Communication Technology Systems purchases for efficient, economical and effective use of resources.

Procedures:

- a) All computer resources acquired by the Authority are the property of the Company and will be operated, maintained and administered by the Company to maximize its benefits.
- b) All ICT systems acquisitions (i.e. computer hardware, computer software) must be coordinated with the Information & Communication Technology System (ICTS) department and must be identified as a priority within the ICT plans of the area, where the plans are derived from:
 - Annual budget inputs
 - Business need analysis
 - Market demand
 - Rapid technology change
- c) Ensure acquisition of hardware from authorized 'brand' dealers and where the CVs of their support team are impressive and possible service and maintenance agreements can be drawn and agreed
- d) Any repair work of the above equipment should be coordinated by ICTS Repair Center.
- e) All computers should be connected to an Uninterruptible Power Supply (UPS) source.
- f) The software must be used for Authority's work only. Only Company **owned and licensed** software should run in LBDA's Systems.
- g) Purchased software should be copied and distributed to relevant users and originals kept under ICTS custody, but should observe the copyright law.
- h) User license regulations and copyright issues should be adhered to.

4.4 Pornography/Hatred

Rationale:

The Authority's believes that it has a social responsibility to provide leadership and follow community standards with respect to the distribution and use of offensive material.

Procedures:

- a) All users are to report any perceived occurrences of offensive material involving the computer resources to a staff member of the Information & Communication Technology Systems (ICTS) or the supervisor.
- b) The appropriate ICTS staff or the supervisor is to review any suspected material in order to determine if it falls within this category and to remove from the computer resources any data, computer programs or other forms of information identified as obscene.

4.5 Physical Security

Rationale:

To protect company computing resources from theft, vandalism, and/or accidental damage.

Procedures:

- a) All computing equipment must have reasonable physical security in place (i.e. reasonable measures to prevent theft and vandalism).
- b) Removal of LBDA's computer resources from the premises must be completed in accordance with the current company procedures for transfer of equipment.
- c) Movement of computer hardware and accessories from one point to another shall be coordinated through Stores In Charge and Head of ICTS, Departmental heads or their appointees. In the case of laptop computers, the department or individual to whom this equipment is assigned is responsible for an appropriate process to control its movements.

4.6 Data Security

Rationale

The Authority will ensure security and integrity of the data and information stored in the computer system.

Procedures

- a) Employees may not sell, reproduce or use company programs or company computer equipment for their own benefit or for unlawful purposes.
- b) No person shall jeopardize the integrity of the computer resources, its operating programs or other stored information.
- c) ICT Systems users should seek appropriate approval to alter, update, or insert Management Information Systems records.
- d) ICTS users should refrain from disclosure of data / information or displaying **insert screens** to unauthorized persons.
- e) All authorized users should guard against misuse of data / information that they may come across in performing their duties.
- f) All printouts should be disposed in an appropriate manner that they cannot be reconstructed easily.
- g) Dissemination of information should be done under signature and to the rightful recipient
- h) ICT Hardware support / agents/ resource personnel should **only** upgrade / replace an operating systems after careful consideration of existing applications
- i) ICT Hardware support / agents/ resource personnel should **only format a HARD DISK** of a workstation i.e. it has 'useful' applications, after consultation with SECTION HEAD of the affected area and head of ICTS.
- j) Sabotage, espionage of Authority's systems, or both, is serious offences where a disciplinary action can be taken against the offender.
- k) Each site to have a heat resistant data safe for backups e.g. local and remote
- l) Servers to be fitted with relevant storage devices e.g. DVD drives/ Flash Disks etc.
- m) ICTS users with access to USB ports, CD R, DVD WRITER devices to apply best practices to avoid 'abuse' of Authority's investments.

4.7 User Privacy

Rationale:

The Company believes that each individual has a right to privacy.

Procedure:

- a) All users must respect each user's right to privacy.
- b) No person, regardless of status (i.e.; including the system manager, or company administrator) may view or change or remove another users files without the user's permission, whether the material exists on a shared computer, network media or on a staff's own media (e.g., a personal flash disk).
- c) E-mail messages are to be treated as private.
- d) Prior to leaving their workstation unattended, users must ensure they are logged out from the network. Lack of system protection does not constitute permission to use it.
- e) Users are to only access accounts to which they have been authorized.
- f) Each user is responsible for maintenance of files on their account. It is necessary for the user to review various documents that exist and remove those that are no longer required.
- g) User privacy must be extended to the computer system itself.
- h) Employees may not install software on to the hard drives or any of the computer networks unless instructed by their supervisor.
- i) Users must immediately report suspected unauthorized use of accounts to their Supervisor or to the Information & Communication Technology Systems (ICTS) staff.
- j) All users must exercise appropriate measures to maintain confidentiality and integrity of any information of confidential nature acquired through computer access.

4.7.1 Privacy - Exceptions.

Files, which reside in a user's account, which exist on a user's own media or the network media are to be considered private except where:

- A runaway program which could be either accidental or intentional hack or a virus is in the process of causing damage or is inhibiting the work of others. In this case it may be necessary for a system manager to inspect the file, which is suspected of causing the problem.

Procedures:

- a) Where user names and/or passwords are instituted in order to provide authorized access, the sharing of these user names and/or passwords with any other individual is prohibited.
- b) Copying or accessing of files and/or directories belonging to other users is prohibited unless authorization is given.

4.8 Server Security

Rationale:

The basis for a secure resilient network with data integrity is network servers managed to the highest standard.

Procedures:

4.8.1 General

- a) There shall be no remote control of the server (i.e. from other than the console) except during troubleshooting.
- b) Similarly, there shall be no remote execution of server functions. All server functions must be done from the console. This excludes access via local workstations other than the server, dial-in, gateways, bridges, routers, and protocol converters.
- c) All administrator operations (e.g. security changes etc) shall be done from console.
- d) Supervisor-level logon shall not be done at any device other than console.
- e) No user programs shall be executed at the server by user initiation.
- f) There shall be no access to the server or to any server resources following a diskette or flash disk boot.
- g) There shall be no peer-to-peer direct communication. All such communication must be done through the server.
- h) There shall be no multiple users Ids passwords logged on (i.e. the same user logged on to the system in two or more locations at a given time). Further, there should be the ability to suspend the active user session and issue alarms should this situation occur.
- i) There shall be no unauthorized or unsupervised use of traffic.

- j) There shall be a formal complete and tested disaster recovery plan in place for all LANs. This should include communications equipment and capabilities in addition to computer, hardware and software.
- k) There shall be no sensitive information ever sent over lines of any sort in clear text format.
- l) Workstations should be suspended after a period of inactivity determined by the LAN administrator, and terminated after a further predetermined period of time has elapsed.
- m) Explicit session (memory cleanup activities should be performed after session disconnect, whether the session disconnect was by workstation request (logoff), by server initiative (such as due to inactivity), or accidental (even if only temporary, as might be the case with a line drop).
- n) In cases where session slippage tends to occur (such as line drops) or in instances where service requests require significant changes of access level privileges, re authentication should be required.
- o) User Ids and passwords should be suspended after a period of disuse specified by the LAN administrator.
- p) Successful logons should display date and time of last logon and logoff.
- q) There should be the ability to disable keyboard activity during specified operations.
- r) The integrity of data should be maintained by using transaction locks on all shared data (both data files and databases).
- s) The integrity of data and the availability of data and the entire LAN should be maintained by specific protections against viruses and other malicious codes.
- t) Only the LAN administrator should make only from the server and all security functions and software changes/additions.

4.8.2 Access Control

- a) The server should be able to require user identification and authentication at times other than logon.
- b) Re-authentication should be required prior to accessing critical resources.
- c) File and directory capabilities should be set in keeping with the sensitivity and uses of the files and directories.
- d) Users should be granted rights and privileges only on a need-to-know/need-to-use basis.

4.8.3 Logging

- a) Audit logs should be kept of unsuccessful logon attempts, authorized access/operation attempts, suspends and accidental or deliberate disconnects, software and security assignment changes, logons/logoffs, other designated activities (e.g., accesses to sensitive files) and, optionally, all activity.
- b) Audit log entries should consist of, at a minimum, resource, action, user, date and time, and (optionally) workstation ID and connecting point.
- c) There should be an automatic audit log review function to examine all postings by posting type (e.g., illegal access attempt, and access of sensitive data). For each posting type, if a threshold set by the LAN administrator is exceeded, an alarm should be issued and an entry made in an action-item report file.
- d) The audit file should be maintained in encrypted format.
- e) There should be reporting functions to readily and clearly provide user profiles and access rules, as well as reports on audit log data.

4.8.4 Disk Use

- a) All programs should be read-only or execute-only, as appropriate to their sensitivity, ownership, licensing agreements and other considerations; and/or should be kept in read-only or execute-only directories. This should also apply to macro libraries.
- b) Users should be provided with private directories for file storage.
- c) There should be no upload of programs to public areas; the same is true for macros and macro libraries.

4.8.5 Backup

The business continuity is paramount. Backup of the data/files from our applications/packages is mandatory.

- a) Automate backup operations, where possible.
- b) Schedule and perform regular / frequent backups. These backups should provide automatic verification (Read-after-write).
- c) Backups should be stored into CD RW or CD R, DVD, Flash disk or secondary hard disks.
- d) Backup should be kept off-premises.
- e) Both backup and restore/recovery functions should be regularly tested
- f) Backups to be stored in heat resistant data safes.
- g) Use Operating Systems backup / restoration suite, applications or Third Party suite to perform backups. Compatibility is important.
- h) Schedules for the backup shall be developed under direction of ITS. Responsibility for taking backups will be specifically assigned.

4.8.6 Communications

- a) Communications access should be restricted to specific users programs, data transaction types, days/dates and times.
- b) An extra layer of identification authentication protocol should be in effect challenge-response, additional passwords, to communications access.
- c) All communications access should be logged.
- d) All communication access messages should be authenticated using message authentication code, digital signature, etc.
- e) The password change interval should be shorter for communications process users.
- f) Stronger encryption algorithms should be used for communication access users.
- g) Any and all confidential information, including passwords and data, should be encrypted during transmissions in either or both directions for all communications access activities.
- h) Encryption capabilities for communications should include both end-to-end and link encryption.

4.8.7 Specific Password Guidelines

- a) Password should require a minimum of at least six characters (eight are preferable, more would be better) and allow a maximum of at most 24 characters (more would be discouraged).
- b) They should be case-sensitive.
- c) There should be a requirement for at least one uppercase character, one lowercase character, one numeric and one alphabetic character. For high-security access, this should be extended to include one non-print (and non-space) character.
- d) Password should be changed frequently. Quarterly is a minimum, monthly is better. High security access should have weekly change.
- e) There should be computer-controlled lists of proscribed password to include common words and standard names, and employee/company information as available (name, address, social security number, license plate number, date of birth, family member names, company departments, divisions, projects, locations, etc). There should be tests (letter and number sequence, character repetition, initials, etc) to identify password weakness.
- f) There should be reuse restrictions so that no user can reuse any of the more recent passwords previously used. Eight is a suggested minimum and more would be better.
- g) There should be no virtual indication of password entry or of password entry requirement. This obviously prohibits the password characters from echoing on the screen.
- h) New passwords should always be entered twice for verification.
- i) Time allowed entering a password, and number of entry attempts should be limited.
- j) Particularly sensitive files, even when encrypted, should require an authentication code (i.e. a second password) for access.
- k) In addition to the password with associated supervisory privileges, each LAN administrator should have an additional password for “**normal**” system use without supervisory privileges.

4.9 Fair Warning

Rationale:

The Authority believes that this policy should be shared in an open and honest manner.

Procedures:

- a) The Security policy must be posted in all high traffic areas.
- b) Where possible, upon start-up of each session, there should be a notification that compliance to a set of standards is required in order to access these resources.
- c) Extracts that concern a category of users can be distributed at inception, or induction.

4.10 Copyright

Rationale:

The company believes that it has a corporate responsibility to protect against the improper use or illegal copying of software.

Procedures:

- a) Must communicate the software copyright protection laws wherever software is distributed.
- b) All copies of software owned by the Authority must contain a label indicating that the software is the property of the Company.
- c) Information & Communication Technology staff will not install any software onto any company computing resource unless a valid license of the software is provided or the staff member is aware that the software license is legal for this resource.
- d) Once Information & Communication Technology staffs are invited onto a user's computer, if they have reason to believe that the copyright laws are being violated, they must request verification of a valid software license for the software on this computer. If it cannot be produced, then the software will be removed until the situation can be resolved.

4.11 Network Expansion and Resource Utilization

Rationale:

Harmonize and coordinate network expansion activities and maximize on resource usage for proper return on investment

Procedures:

ICTS Department Head shall be responsible for the coordination of all network expansion activities and optimum resource utilization. This includes but is not limited to the following:

- a) Maintenance and repair of network resources
- b) Creating new users on the network. This responsibility may be delegated as necessary.
- c) Requisition of hardware and/or software.
- d) Liberty to relocate any resource deemed underutilized.
- e) Identify and advise the company on computer hardware/accessories/software that should be disposed.

4.12 Purpose of Use

Rationale:

The company believes that all computing resources should be available on a company-wide basis and should be used for the sole purpose of the Authority's business or related activities.

Procedures:

- a) Any use of company resources for personal gain is discouraged.
- b) Report any actions contrary to these policies to the appropriate Section head or Information & Communication Technology Systems (ITCS) Centre.
- c) Suspected misuse of computing resources should be reported to ICTS centre for follow-up.
- d) Printers should not be simply used as photocopiers. Need to recognize the effectiveness of the printers versus the photocopiers and how each should be used.
- e) Due to the company's commitment to staff professional development and career advancement, preparation of resumes and application cover letters are allowed on the company's computer resources.
- f) User must refrain from engaging in deliberately wasteful practices such as:
 - Unnecessary printings
 - Unnecessary holding of devices or telecommunication lines
 - Creation and retention of unnecessary files.
 - Non-office related activities such as banners, signs, sport pools, games etc. which consume computing resources are not allowed.

4.13 Viruses/worms/Spy ware

Rationale:

Viruses can destroy hardware, operating systems and applications and worms/spy ware can cause disturbance, annoyance, delay processing and connectivity.

Procedures:

- a) The Authority should strive to purchase a powerful, high quality anti-virus and firewall programs to curb menace
- b) ICTS users should run anti-virus program immediately after computer start-up, in case the anti-virus program is not configured to run at start-up.
- c) Anti-virus programs should be installed and configured by competent ICTS personnel so as to include all necessary options e.g. action to be taken when virus (es) is/are detected.
- d) ICTS support **SHOULD** perform routine checks and file a report about the workstation virus-status on quarterly basis.
- e) Effort should be made to update anti-virus program on weekly **but not beyond a month.**
- f) Disabling of some hardware devices maybe encouraged where guidelines are ignored and virus attack is rampant.
- g) Installations of non-vetted screen savers, games and trial processing programs are highly discouraged.
- h) Floppy diskette, Flash disks movement is discouraged and if necessary must be scanned.
- i) ICTS users should report all detected viruses to ICTS Centre or office.
- j) ICTS users should exercise extreme care to avoid diskette or flash disk **boot up scenario.** Remove all floppy diskettes and flash disks **immediately** after use.

5 NON-COMPLIANCE

- a) The first incidence of non-compliance to this policy will result in a written warning by ICTS or authorized agents, copied to controlling officer or management.
- b) The second incidence of non-compliance will result in a loss of use of all computer privileges. It is understood that the second incidence may not necessarily be of the same type as the first. At this point disciplinary action will be taken by the Administration Department or Controlling officer.
- c) It should be noted that in specific instances, due to the severity of the offence, serious disciplinary action will be taken immediately.
- d) The Information & Communication Technology Systems (ICTS) staff performs their duties with the understanding that any breach of security or illegal activity that they are knowingly involved in means immediate disciplinary action.
- e) The consequences for non-compliance will usually be the suspension of access and may include probation, suspension from LBDA or in the case of a salaried employee, even termination or legal action.

6 Due Process

- a) All due process rights as stated in each individual's contract with the Company will be honoured. Staff members are protected by their specific Labour Agreements as published in the terms and conditions of service.
- b) Due Process - Statement of Exemption

The special exception is intended to protect the property, health, safety and well being of an accused or another member of the Company.

This exception is extended in some cases to cause immediate suspension of computer access. For example, a case in which a user is intentionally causing sweeping destruction or is inhibiting work for other users and for which an immediate suspension of access is the only remedy because the accused refuses to terminate the process or the accused has clearly set it into an autonomous state; in other words, in an emergency. In this case, access may be suspended immediately and the accused will be notified as soon as possible and has the right to a hearing within seventy-two hours of being notified or such other time as may be allowed by the Human Resources Department regulations and guidelines.

7 Specific Proscriptions:

It is important to note that in a modern organization users are learning as they work and errors occur which may cause system disruption and that ordinary errors of this type are certainly beyond the scope of inappropriate use. For example, a poorly written, runaway C program is not necessarily a violation. It may be an accident. The intent of the user is the critical point.

Specific examples of inappropriate uses of LBDA's computing facilities include but are not limited to:

- a) Gratuitous use of resources such as CPU time or disk space with the intent of slowing the overall system or obstructing the work of others.
- b) Copying licensed software from lab micros or from the multi-user systems for personal use is considered theft.
- c) Intentionally crashing a computer, network or printer or intentionally making them difficult to access or use.
- d) Erasing or changing another user's files or computer environment without the user's permission.
- e) Causing a user's disk quota to be exhausted and thereby preventing the individual from working effectively: for example, 'mail bombing' someone with a deluge of unsolicited messages. The content of the messages is irrelevant; it is the intent to inhibit productivity or damage a user's environment, which is of issue here.
- f) Adding unauthorized software to shared company computers is not permitted. The intent of this Statement is largely to maintain a stable environment for users. Adding a game, for example is unacceptable. Adding a statistical package is also unacceptable because it also can disrupt the operation of the computer for others. However, we are willing to review and approve exceptions in a timely way. Simply contact any member of the Network Support Team.
- g) Intentionally modifying computer interfaces (the look of the screen) so that the machine becomes difficult or impossible to use. For example, removing programs or scrambling the icons on a Windows, Macintosh or server computer.
- h) Unauthorized use of company facilities, including buildings, grounds and equipment. Computing facilities are only for the use of LBDA staff as well as visitors who have applied for access.
- i) Use of the facility by unauthorized individuals. Computer accounts and IDs are not to be shared.
- j) Acquiring files for the purpose of using them or reading them when it is clear that the file(s) are intended to be erased. Some systems cannot

absolutely guarantee that files are destroyed once deleted and the intentional recovery of someone else's deleted files is construed to be unauthorized access and a violation of rights of privacy.

- k) Intentionally acquiring privileges or rights in a system which is normally beyond the scope of the user; for example obtaining system administrator access to a system or gaining operator rights or discovering another user's password and using it to gain access to the user's personal account on a shared system.
- l) Electronic eavesdropping or tapping the network or another computer. The exception is where the system manager must inspect network or system transmissions for purposes of diagnosis or maintenance. In this case, only protocol and not message contents (detail) will be observed.
- m) Selling access to LBDA's computing facilities. You may not lease, loan or barter Authority's computing equipment.
- n) The use of LBDA's computer facilities to attack other systems at LBDA's or anywhere in the world (the Internet or any associated network or personal computer)