Information Technology

Policy Document

Policy Document Version Control

Change Record

Date	Author	Version	Changes
November 2021	PIC	0.0	Zero Draft
6 Jan 2022	Daud Suleman	0.1	Zero Draft

Review Record

Date	Reviewer	Version
	PIC Review	0.2
	DOX Review	0.3
	Committee Review	0.4
	Board Approval	1.0

Approval Record

Date	Approved By	Version
	Board Approval	

Copyright Protection

Table of Contents

1 Introduction

1.1 Intent of IT Policy

This policy intends to establish guidelines for the employees using MACRA's computing facilities, including computer hardware, printers, software, e-mail, and Internet and collectively called "Information Technology".

1.2 Purpose of IT Policy

All employees share the Information Technology facilities at MACRA. These facilities are provided to employees to conduct MACRA's business. MACRA does permit a limited amount of personal use of these facilities, including computers, printers, e-mail, and Internet access. However, these facilities must be used responsibly by everyone, since misuse by even a few individuals has the potential to negatively impact productivity, disrupt MACRA's business, and interfere with the work or rights of others. Therefore, all employees are expected to exercise responsible and ethical behavior when using MACRA's Information Technology facilities. Any action that may expose MACRA to risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

1.3 Compliance with IT Policy

The use of MACRA's information technology facilities in connection with the Authority business and limited personal use is a privilege but not a right, extended to various Authority employees. Users of MACRA's computing facilities are required to comply with all policies referred to in this document.

Users also agree to comply with applicable national laws and to refrain from engaging in any activity that would subject the Authority to any liability. MACRA reserves the right to amend these policies and practices at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with applicable national laws.

To protect the integrity of MACRA's computing facilities and its users against unauthorized or improper use of those facilities, and to investigate the possible use of those facilities in violation of Authority rules and policies, MACRA reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine the authorized use of any computing facility or which is used in violation of Authority rules or policies. MACRA also reserves the right periodically to examine any system and other usage and authorization history as necessary to protect its computing facilities.

MACRA disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

1.4 Scope of IT Policy

This policy applies to all MACRA employees and all employees of MACRA’s affiliates. It is the responsibility of all operating units to ensure that these policies are communicated, understood, and followed.

These policies also apply to software contractors, and vendors/suppliers providing services to MACRA that bring them into contact with MACRA’s Information Technology infrastructure.

These policies cover the usage of all of the Authority’s Information Technology and communication resources, including, but not limited to:

- All computer-related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, mobile telephones, wireless computing devices, telecom equipment, networks, databases, printers, servers, and shared computers, and all networks and hardware to which this equipment is connected.

- All electronic communications equipment, including telephones, pagers, radio communicators, voice-mail, email, fax machines, wired or wireless communications devices and services, Internet and intranet, and other online services.

- All software including purchased or licensed business software applications, Authority-written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on Authority-owned equipment.

- All intellectual property and other data stored on MACRA's equipment.

- All of the above are included whether they are owned or leased by the Authority or are under the Authority's possession, custody, or control.

These policies also apply to all users, whether on Authority property, connected from remote via any networked connection, or using Authority equipment

1.5 Updating of IT Policy

This policy is not a static document. It is a dynamic document that would need to be updated according to business needs, technology trends, and MACRA's strategy.

All changes made to this Policy document should be thoroughly recorded under the Policy Document Version Control section.

This policy should be reviewed at least once annually and as technological changes demand.

Changes to the IT Policies should be endorsed by the Project Implementation Committee (PIC), Senior Management of MACRA, and finally the respective committee of the Board before the policies become binding.

1.6 Potential Disciplinary Action:

Failure to comply with MACRA policy may result in disciplinary action including but not limited to the loss of applicable corporate privileges or more severe disciplinary actions including employment termination.

2 POLICIES

2.1 Policy Management

2.1.1 Information Technology Steering Committee

Until further notice, an IT Steering committee or its equivalent must be composed of at least the following:

- Director Legal
- Head of IT
- Director Telecoms
- The Head of Internal Audit
- The Head of Risk
- The Finance Manager

This committee will meet regularly to:

- Review the current status of MACRA's information security, evaluate and score MACRA's information security and efficiency
- Approve and later review IT projects
- Approve new or modified IT policies

A detailed charter outlining the terms of reference for the IT Steering committee shall be maintained at all times.

2.1.2 Information Ownership and Management's Responsibilities

All production information possessed by or used by MACRA must have a designated owner.

- Owners must determine appropriate sensitivity classifications as well as criticality ratings.
- Owners must make decisions about who will be permitted to access the information, and the uses to which this information will be put.

- Owners must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.
- Any change in the present Policy manual must be approved by the Board.

2.1.3 Control Implementations Consistent With MACRA Standard

Management is responsible for implementing information system controls in a manner that is consistent with MACRA standards and local legal requirements.

2.1.4 Legal Framework For Information Security Policies

MACRA acknowledges the complexity of legal requirements in MACRA's country and International Laws. If any of MACRA's information security policy is believed to be in conflict with existing laws or regulations, this observation must be promptly reported to the IT Steering committee.

2.1.5 Risk Acceptance Process And Permissible Exceptions To Policies

Exceptions to information security policies will be permitted in rare instances where a risk analysis examining the implications of being out of compliance has been performed, where a standard risk acceptance request has been prepared by the responsible manager, and where this request has been approved by the IT Steering committee.

2.2 Password Security

2.2.1 Minimum Password Length

The length of the password must always be checked automatically at the time that users construct or select them. All passwords must have at least eight (8) characters.

2.2.2 Passwords Must Be Difficult To Guess

All user-chosen passwords for computers and networks must be difficult to guess. This means that passwords must not be related to one’s job or personal life. For example, a car license number, a spouse’s name, or fragments of an address must not be used.

This also means passwords must not be a word found in any dictionary or some part of speech. For example, proper names, places, technical terms, and slang must not be used.

Users must be trained in how to select strong passwords. After receiving the training, users must sign a statement undertaking not to choose easy-to-guess passwords, even for software that permit such passwords to be used.

Where software controls permit, users must be prevented from selecting easily guessed passwords.

2.2.3 Passwords Must Not Be Cyclical

Users are prohibited from constructing fixed passwords by combining a set of characters that do not change, with a set of characters that predictably change.

In these prohibited passwords, characters that change are typically based on the month, a department, a project, or some other easily guessed factor. For example, users must not employ passwords like “X34JAN” in January, “X34FEB” in February.

2.2.4 Passwords Must Contain Both Alphabetic And Non-Alphabetic Characters

All user-chosen passwords must contain at least one alphabetic and one non-alphabetic character. Nonalphabetic characters include numbers (0-9) and punctuation and other symbols (e.g. !, ”, #, $, %, &).

The use of control characters and other non-printing characters is discouraged because they may inadvertently cause network transmission problems or unintentionally invoke certain system utilities.

2.2.5 Reset Required For Users Who Forget Passwords

Users who forget or misplace their password must request the IT Department to reset the existing password.

2.2.6 Different Systems Must Use Different Passwords

Users must not use the same password on multiple computer systems unless the user signs a responsibility statement for each computer system or application.

Should MACRA engage the use of single sign-on (SON) devices and technologies, the policy shall be exempted as all logins shall be managed from one place.

2.2.7 Suspected Disclosure Forces Password Changes

All passwords must be promptly changed if they are suspected of having been disclosed, or known to have been disclosed, to unauthorized parties.

2.2.8 Storage Of User Passwords

Passwords must not be written down in any place where unauthorized persons might discover them.

Users must not write down or otherwise record a readable password and store it near the access device to which it pertains. For example, a personal identification number (PIN) must never be written down on an automated teller machine (ATM) card.

2.2.9 Passwords Must Not Be Shared

Access control to files, applications, databases, computers, networks, and other system resources via shared access or common passwords is prohibited.

Regardless of the circumstances, passwords must never be revealed to anyone besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password.

If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms.

2.2.10 Users Responsible For All Activities Involving Personal User IDs and Passwords

Users are responsible for all activities performed with their personal user IDs and passwords. User IDs may not be utilized by anyone but the individuals to whom they have been issued.

Users must not allow others to perform any activity with their user IDs.

Users are forbidden from performing any activity with IDs belonging to other users.

2.2.11 Password History Must Be Maintained

On all multi-user machines, system software or locally developed software must be used to maintain an encrypted history of previously fixed passwords. This history file must be employed to prevent users from reusing it. The history file must minimally contain the last three (3) passwords for each user ID.

2.2.12 Periodic Forced Password Changes

All users must be automatically forced to change their passwords at least once every ninety (90) days.

2.2.13 Limit On Consecutive Unsuccessful Attempts To Enter A Password

To prevent password-guessing by unauthorized users, the number of consecutive attempts to enter a password correctly must be limited to three (3) attempts.

After three unsuccessful attempts to enter a password, the involved user ID must be either (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than sixty minutes, or (c) if dial-up or other external network connections are involved, it must be disconnected.

2.2.14 Passwords Must Not Be Displayed Or Printed

The display and printing of passwords must be masked, suppressed or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.

2.2.15 Protection Of Passwords Sent Through The Mail Or Email

If sent by regular mail or email, passwords must be sent separately from user IDs. These messages must have no markings indicating the nature of the enclosure.

If sent by regular mail, passwords must be concealed inside a secured, tamper-proof envelope like PIN or Password Mailer that will readily reveal tampering.

If sent by email, passwords should be sent in an encrypted, password-protected zip or rar file attached to the message. The password for the zip or rar file should be sent via a different medium (e.g. by telephone call).

2.2.16 Storage Of Passwords Must Not Be In Readable Form

Passwords must not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access controls, or in other locations where authorized persons might discover or use them.

2.2.17 Encryption Of Passwords

Passwords must always be encrypted when held in storage for any significant period of time or when transmitted over networks, communication facilities, or any form of electronic transmissions. This will prevent them from being disclosed to wiretappers, technical staff who are reading system logs, and other unauthorized parties.

2.2.18 Incorporation Of Passwords Into Software

To allow passwords to be changed when needed, passwords must never be hard-coded (incorporated) into software developed by or modified by MACRA personnel or external consultants.

2.2.19 Prevention Of Password Retrieval

Computer and communication systems must be designed, tested, and controlled so as to prevent the retrieval and unauthorized use of stored passwords, whether the passwords appear in encrypted or unencrypted form.

2.2.20 Passwords For Internal Network Devices

Categories of devices on MACRA's internal network (e.g. routers, firewalls, access control servers) must have the same password or other access control mechanisms to facilitate efficient management of the devices. The parameters of the password of the devices must adhere to policies in this section.

The passwords for the devices must be changed every 90 days and a log of the password change must be kept. The log must be signed off by the implementer of the password change, the ICT Infrastructure Manager, and the Head of IT.

2.2.21 Vendor Default Passwords Must Be Changed

All vendor-supplied default passwords must be changed before any computer, communications system or software is used for MACRA's business.

2.2.22 Administrator's Password Common to All Workstations

All workstations must have a common local administrator password, to avoid problems and delays during the set-up of devices and applications.

2.2.23 Administrator's Password, Security Keys and Other Access Codes Controllership

The administrator password must be controlled primarily by the Head of IT and the appointed Systems Administrator(s).

Setting this password is the responsibility of the Head of IT.

Where management of the systems is outsourced, the administrator password must be controlled and approved by the outsourcing entity.

2.2.24 Storage of Administrator Passwords, Security Keys, And Other Access Code

Administrator passwords, security keys, and access codes must be stored in hard copy form, sealed individually in an envelope, with the signature of the designated officers across the seal.

A Control List must be maintained to control the inventory of passwords, security keys, and other access codes.

Administrator passwords, security keys, and other access codes must be stored in a safe deposit box of MACRA’s vault.

A copy of the administrator passwords, security keys, and other access codes must be stored in a secure location outside MACRA’s premises, such as in a safe deposit box in another MACRA’s vault.

2.2.25 Responsibility Statement For Use Of Administrator Rights

Any worker who uses passwords, security keys, and other access codes with administrator rights or its access equivalent must sign a responsibility statement.

2.2.26 Forced Change Of All Passwords

Whenever a system has been compromised by an intruder or is suspected of having been compromised, system managers must immediately change every password on the system involved.

Under either of these circumstances, a trusted version of the operating system and all security-related software must also be reloaded.

Under either of these circumstances, all recent changes to user and system privileges must be reviewed for unauthorized modifications.

2.2.27 Transfer Of User To Other Branch Or Department

When a user is transferred to a new department or branch, the HR department is responsible for informing the IT department of the change before it occurs, so that the user ID and password of the user can be reassigned at the time of the change.

2.3 Login Process Controls

2.3.1 Unique User IDs and Password Required

Every user must have a single unique user ID and personal secret password. This user ID and password will be required for access to MACRA's multi-user computers and computer networks.

2.3.2 Anonymous User IDs Must Not Be Used

Anonymous user IDs must not be assigned to users.

Guest user IDs must always be disabled.

All user IDs must identify their owner. The user ID should use the first name of the owner's given name, and surname. For example, for John Phiri, the user ID must be "john.phiri".

2.3.3 Automatic Log-off Process

If there has been no activity on a computer terminal, workstation, or PC for ten (10) minutes, the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided the proper password. This is valid for both OS and main applications (CIRMS, AccPac, etc).

2.3.4 Logging-Off PC Connected To Networks

If personal computers (PCs) are connected to a network, when unattended the connection must always be terminated by the system automatically.

2.4 Access Controls

2.4.1 System Logout Or Locking

Users must log out of a computer before leaving it, or lock the computer if they are leaving the computer for a short time.

2.4.2 Browsing On MACRA Systems and Networks Prohibited

Workers must not browse through MACRA computer systems or networks. For example, curious searching for interesting files and/or programs in the directories of other users is prohibited. Steps taken to legitimately locate information needed to perform one's job are not considered browsing.

2.4.3 Resignation And Suspension Of Employment Mean Termination And Suspension Of Access

When a worker resigns or is dismissed, the HR department is responsible for informing the IT Department immediately.

IT staff must suspend the worker's access rights immediately on receiving the notice from the HR department, or at any later time requested by the HR department.

The worker's user ID will remain suspended for 30 days so that data can be re-assigned to other workers. After 30 days, access will be terminated.

2.4.4 Gaining Unauthorized Access Via MACRA Information Systems

Workers using MACRA information systems must not attempt to gain unauthorized access to any other information systems, or in any way damage, alter, or disrupt the operations of the systems. Likewise, workers must not capture or otherwise obtain passwords, encryption keys, access cards, or any other electronic control mechanism, which could permit unauthorized entry.

2.4.5 Access To MACRA Systems For Third Parties With A Contract

Before a third party is given access to MACRA systems, a contract defining the terms and conditions of such access must have been signed by authorized persons at the third party organization.

MACRA Head of IT must also approve these terms and conditions.

2.4.6 Access To MACRA Systems For Third Parties Without A Contract

Individuals who are not employees, contractors, or consultants may be granted a user ID or otherwise be given privileges to use MACRA's computers or communications systems at the written request of a department head.

The department head making the request is responsible for the use of MACRA's systems made by the third party.

Third parties given access under these conditions must follow the rules on password handling and user ID requirements specified in this document.

Third-party user IDs must be suspended or terminated when not in use.

2.5 User Controls

2.5.1 User Privileges Definition

Management must define user privileges such that ordinary users cannot gain access to, or otherwise interfere with, either the individual activities or the private data of other users.

Users must not read, modify, delete, or copy a file belonging to another user without first obtaining permission from the owner of the file. Unless general user access is clearly provided, the ability to read, modify, delete or copy a file belonging to another user does not imply permission to actually perform these activities.

Without specific written approval from management, administrators must not grant privileges beyond the user's job functions and responsibilities.

All user ID creation, deletion, and privilege change activity performed by systems administrators and others with privileged user IDs must be securely logged and must be available for audit.

2.5.2 Separation of Duties And Control Over MACRA Assets

Whenever MACRA computer-based process involves sensitive, valuable, or critical information, the system must include controls involving separation of duties or other compensating control measures. These control measures must ensure that no individual has exclusive control over these types of MACRA information assets.

Wherever practical, no person should be responsible for completing any task involving sensitive, valuable, or critical information from beginning to end. Likewise, a single person must not be responsible for approving their own work. Wherever possible, every task involving sensitive, valuable, or critical information must require at least two people to coordinate their information-handling activities.

2.5.3 Production Business Information Controls

System privileges must be defined so that non-production staff (internal auditors, information security officers, programmers, computer operators, etc.) are not permitted to update production business information.

2.5.4 Time-Dependent Access Control

User activities must be restricted by time and day of the week. For example, time restrictions must be set up in CIRMS to automatically log off the user when his/her working hours end during the day.

2.5.5 Access To Sensitive Information

Workers who have been authorized to view information classified at a certain sensitivity level must be permitted to access only the information at this level and at less sensitive levels.

Workers must not move information classified at a certain sensitivity level to a less sensitive level unless this action is a formal part of an approved reclassification process.

2.5.6 Reporting Changes In User Duties

The HR Department must report all significant changes in work duties or employment status to the IT Department before those changes occur so that access privileges for the affected users can be changed at the correct time.

2.5.7 Database Updates Must Be Made Only Through Established Channels

Updates to production databases must only be made through established channels, which have been approved by management. The use of direct database access utilities in the production environment is not permitted unless specifically approved by the management, because these programs will circumvent database synchronization and replication routines, input error checking routines, and other important control measures.

2.5.8 User Access To System Commands

After logging in, all users of multi-user systems must be restricted to using menus, which show the options that they have been authorized to select. The user must not be allowed to invoke system-level commands. The user must be presented with only the system capabilities and commands that they have privileges to perform.

2.5.9 No Unauthorized Testing Of Information System Controls

Workers must not test or attempt to compromise internal controls unless justified with legal purpose and specifically approved in advance and in writing by the Head of IT.

2.5.10 Restricted Remote Administration Of Internet–Connected Computers

Remote administration of Internet-connected computers is not allowed unless passwords are employed over encrypted links.

2.6 System administration - controls

Every MACRA multi-user computer system must have a designated security administrator to define user privileges, monitor access control logs, and perform similar activities. For purposes of this policy, local area networks (LAN), Wide area networks (WAN), servers, security and alarm systems, and private branch exchange (PBX) switches are considered to be multi-user systems.

2.6.1 Risk Assessments Required For Production Systems Designated Security Administrator For All Multi-User Systems

All production computer information systems must be periodically evaluated by the IT Department, and Internal Audit to determine the minimum set of controls required to reduce risk to an acceptable level.

Information systems security risk assessments for critical information systems and critical production applications must be performed at least once a year. All major enhancements, upgrades, conversions, and related changes associated with these systems or applications must be preceded by a risk assessment.

2.6.2 Security Requirements For Third Party Contracts

All agreements dealing with the handling of MACRA information by third parties must include special clauses. These clauses must allow MACRA to verify the controls used for these information-handling activities, and to specify the ways in which MACRA information will be protected. MACRA's business partners, suppliers, customers, and other business associates must be made aware of their information security responsibilities via specific language appearing in contracts that define their relationship with MACRA.

All information-systems-related outsourcing contracts must be reviewed and approved by the management. It is the Head of IT responsibility to make sure that these contracts sufficiently define information security responsibilities, as well as how to respond to a variety of potential security problems. It is also the Head of IT's responsibility to make sure that all such contracts allow MACRA to terminate the contract for cause if it can be shown that the outsourcing firm does not abide by the information security terms and conditions of the contract.

Before any third-party users are permitted to reach MACRA systems via real-time computer connections, specific written approval of the DG or Head of IT (depending on the type of permission and the level of risk involved) is required. Request for approval must specify the security-related responsibilities of MACRA, the security-related responsibilities of the common carrier (if used), and the security-related responsibilities of all other involved third parties. These responsibility statements must also address the liability exposures of the involved parties.

2.6.3 Authorized System Administrator Examination of Private User Files

Systems administrators are authorized to examine private user files to handle emergencies such as virus infestations and system crashes. Whenever user files are examined in this manner, the involved user(s) must be notified. After the problem has been resolved, all copies of such files made by the administrator must be promptly destroyed.

2.6.4 Logs Required On Application Systems Handling Sensitive Information

All production application systems which handle sensitive information of MACRA must generate logs that show every addition, modification, and deletion to such sensitive information.

All computer systems running MACRA’s production application systems must include logs that record, at a minimum, the following data:

- User session activity includes user IDs, log-in date and time, logout date and time, and applications invoked.
- Changes to critical application system files.
- Additions and changes to the privileges of users.
- System start-ups and shut-downs.

2.6.5 Computer System Logs Must Support Audits

Logs of events relevant to computer security must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with, security measures.

2.6.6 Required Retention Period of Logs

Computerized logs containing events relevant to computer security must be retained for at least two (2) years. The archiving policy should be followed according to the country-specific requirements and data type. During this period, such logs must be secured so that they cannot be modified, and so that they can be read-only by authorized persons. These logs are important for error correction, forensic auditing, security breach investigations, and related efforts.

2.6.7 Persons Authorized to View Logs

All system and application logs must be maintained in a form that cannot readily be reviewed by unauthorized persons. A person is unauthorized if he or she is not a member of the internal audit/risk staff, systems management staff, or if he or she does not clearly have a need for such access to perform regular duties.

Unauthorized users must obtain written permission from the management prior to being granted such access.

2.6.8 Regular Review of System Security Audit Logs

To allow proper remedial action, the IT Department must review records of security-relevant events on multiuser machines every month, or more often as necessary.

2.6.9 Separation Between Production And Development/Test Environments

Business application software in development must be kept strictly separate from production application software. This separation must be achieved via physically separate computer systems. Recommendation: the development/test software can be kept on the backup server.

2.7 Systems Usage Controls

2.7.1 Permissible Uses Of Authority Information

MACRA's information must be used only for business purposes expressly authorized by the management.

2.7.2 Personal Use Of Computer And Communication Systems

MACRA's computer and communication systems must be used for business purposes only. Personal use is only allowed by special permission on a case-to-case basis.

2.7.3 Right To Free Speech Does Not Apply To Authority Systems

MACRA computer and communications systems are not intended for, and must not be used for, the exercise of the participants' right to free speech. Management reserves the right to censor any data posted to MACRA computers or networks. These facilities are private business systems, and not public forums, and as such do not provide freedom of speech.

2.7.4 Right Of Management To Examine Data Stored On MACRA's Systems

All messages sent over MACRA's computer and communications systems are the property of MACRA. To properly maintain and manage this property, management reserves the right to examine all information stored in or transmitted by these systems. Since MACRA's computer and communication systems must be used for business purposes only, workers should have no expectation of privacy associated with the information they store in or send through these systems.

2.7.5 Right To Remove Offensive Materials Without Warning

MACRA retains the right to remove from its information systems any material it views as offensive or potentially illegal, without notice.

2.7.6 Disclosure Of Information On MACRA's Systems To Law Enforcement

By making use of MACRA's systems, users consent to all information they store on MACRA's systems to be divulged to law enforcement at the discretion of MACRA's management.

2.7.7 Games May Not Be Stored Or Used On MACRA's Computer Systems

Games may not be stored on any computer system of MACRA. Any games found on any of the Authority's computers or servers will be uninstalled and/or deleted without notice.

2.7.8 Music Files Must Not Be Stored Or Used On MACRA's Computer Systems

Music files must not be stored on any of MACRA's computers in public contact areas.

Non-work-related music files must not be stored on any of MACRA's servers. This includes user folders stored on servers but accessed from user workstations.

Music files found in unauthorized locations, or found to have been obtained illegally, will be deleted without notice.

2.7.9 Video Files Must Not Be Stored Or Used On MACRA's Computer Systems

Video files must not be stored on any of MACRA's computers in public contact areas.

Non-work-related video files must not be stored on any of MACRA's servers. This includes user folders stored on servers but accessed from user workstations.

Video files found in unauthorized locations, or found to have been obtained illegally, will be deleted without notice.

2.7.10 Disclaimer Of Responsibility For Damage To Data And Programs

MACRA uses controls and other security measures to protect confidentiality, integrity, and availability of the information handled by computers and communication systems. MACRA disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

2.8 Software Controls

2.8.1 Acquisition, Installation, And Registration

Acquisition of software from third-party vendors should pass through an evaluation process by the Internal Procurement committee for its relevance to the operations of MACRA.

There must be at least three short-listed providers to evaluate.

For the acquisition of third-party software, management must obtain a written integrity statement from the involved vendor. This statement must provide assurances that the software in question does not contain undocumented features, does not contain hidden mechanisms that could be used to compromise the software's security, and will not require modification or abandonment of controls found in the operating system under which it runs.

Contracting of Third Parties will be done in line with MACRA's Procurement Policy.

Installation of software must be approved by the Head of IT, to prevent malicious software attacks, system spying, configuration conflicts, and other problems associated with installation. In case of outsourcing the management of the systems, the outsourcing entity must co-approve the installation of the software.

All software acquired from third parties should be registered via the Internet, by phone, or by mail. Registration will accrue certain benefits offered by software vendors, such as free upgrades, security updates, technical support, and promotions.

Documentation, licensing agreements, warranties, manuals, and guides, and after-sales support are primary requirements for third-party software.

2.8.2 Development And Documentation

In-house developed software should pass through a pre-evaluation process and standard developing procedure, including the use of standard coding systems, database management systems, naming standards, and other forms of standardization accepted by MACRA or as adopted by MACRA.

Before a new system is developed or acquired, the business and IT teams must have clearly specified the relevant requirements. Alternatives must be reviewed by the management with the developers and/or vendors so that an appropriate balance is struck between security and other objectives (ease of use, operational simplicity, ability to upgrade, acceptable cost, etc).

Once developed, the system should pass through a testing process, followed by a dry run test. Dry run testing involves all the users of the system and those indirectly affected by the new system.

If an external consultant is hired to do the development, the following steps must be followed:

- Provide clear business requirements to the external consultant.
- Sign a TOR with the cost estimate, clear deliverables, and deadlines.
- The IT Department must make sure that the development is delivered with the source code (if specified in the contract/TOR) and proper technical and user documentation.
- The IT Department must install the development and do the testing on a machine other than the production machine.
- Users must test the development and sign a UAT form.
- The respective business department must ensure that the proper manuals and training are delivered to the users.
- The management must check that all the deliverables specified in the TOR/contract are provided before the final payment is made.

Complete documentation is required including coding procedures, database definition, and systems flow.

Management must ensure that all software developed, and software maintenance activities performed by in-house staff subscribe to MACRA policies, standards, procedures, and other systems development conventions.

Every user who develops or implements software and/or hardware to be used for MACRA business activities must document the system in advance of its deployment. The documentation must be written so that the system may be run by persons unacquainted with it. Such documentation must be prepared even when standard software—such as a spreadsheet program—is employed. Documentation must cover both business and technical references.

2.8.3 Keeping Security Functionality Out Of Business Applications

Whenever feasible and cost-effective, system developers must rely on existing system security functionality rather than incorporating such functionality into applications. Examples of system services include operating systems, network operating systems, database management systems, access control packages, front-end processors, firewalls, gateways, and routers.

2.8.4 Software Licensing Agreements

The agreements for all computer programs licensed from third parties must be periodically reviewed by MACRA's compliance or Internal Audit department.

Whenever bundled systems are being procured, the source must provide written evidence of the software license conveyed.

Third-party software in the possession of MACRA must not be copied unless such copying is consistent with relevant license agreements and either: (a) management has previously approved of such copying, or (b) copies are being made for contingency planning purposes.

MACRA provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendors for additional licensed copies, if and when additional copies are needed for business activities.

Third-party copyrighted information or software, that MACRA does not have specific approval to store and/or use, must not be stored in MACRA's systems or networks. System administrators will remove such information and software unless authorization from the rightful owner(s) can be provided by the involved users.

2.8.5 Unlicensed Application Programs Must Not Be Installed

All small systems (client/server systems, local area networks, personal computers, etc.) must use approved software license management software. Besides detecting unauthorized copies of third-party software, these license management systems must be configured to detect new and/or modified application programs developed by users. In the event of using unlicensed software, MACRA may be exposed to legal problems and copyright violations.

2.8.6 Testing Of Software And Information Prior To User Distribution

Prior to distributing any software or information in the computerized form to MACRA's users, the Head of IT must first have subjected the software or information in question to appropriate testing, including comprehensive scanning to identify the presence of computer viruses.

All software testing should be done on a separate machine (e.g. test environment or backup server).

Executable modules must never be moved directly from test libraries to production libraries. Fully-tested modules must be reviewed and recompiled before being moved into production libraries. Review and recompilation activities must be performed by technical staff not associated with the testing process. This process will help to detect and eradicate errors as well as unauthorized code.

2.8.7 Disabling and Removing Unnecessary Software Features At Installation Time

Software features which could be used to compromise security, and which are clearly unnecessary in the MACRA computing environment must be disabled at the time when software on multi-user systems is installed.

All systems software that will definitely not be used at the present time, and which comes along with the operating system or other systems software, should be removed from production systems at the time when the operating system or other systems software is installed.

2.8.8 User Installation Or Upgrading Of Software On Personal Computers Is Prohibited

Users must not install software on their personal computers, network servers, or other machines without first receiving advance authorization to do so from the Head of IT.

Users are prohibited from installing new or upgraded programs on their workstations. This process will instead be done centrally by systems administrators through an automatic network download or authorized by the Head of IT.

2.8.9 Rapid Roll-Back To Prior Versions Of Production Software

Adequate "rollback" procedures must be developed for all changes to production systems software and production application software. "Rollback" procedures allow data processing activities to quickly and expediently revert to the prior version of such software so that business activities can continue.

2.8.10 Required Reporting Of Software Malfunctions

The users must report all software malfunctions to the IT Department or the line of management, using the helpdesk system.

The IT Department must promptly report all software malfunctions to the supplier, vendor, or helpdesk provider, for action and solutions to avoid disruption of MACRA operations.

2.8.11 Formal Change Control Process Required For Business Applications

A formal written change control process must be used to ensure that all business application software that is in development moves into production only after receiving proper authorization from both IT and the business department.

Prior to upgrades, new or different versions of the operating system and related systems software for the multi-use production computers must go through the testing and change control process.

2.8.12 Use Of Most Current Computer Operating System Versions, Patches, And Updates

To take advantage of the most recent security improvements and products enhancements, MACRA must use the most recent version of all multi-user computer operating systems. Any updates must be applied immediately after testing.

2.8.13 Latest Software Release On Systems Interfacing External Networks

To help ensure that attackers cannot utilize the newest penetration methods against MACRA's systems, all systems interfacing external networks (Internet firewalls, internet commerce server, dial-up MACRA, etc.) must be running the latest versions of the vendor-supplied operating software.

No production server that has production business applications on a centralized database should be interfaced with external networks for which no contract or agreement exists.

2.8.14 Recording And Keeping The Manual And Guide

Software licenses, manuals, guides, drivers, and other documentation must be kept in the form of a library or in MACRA's (or IT) Library for safe-keeping, monitoring, and inventory control.

2.8.15 Review Of Invoices From IT Service Providers

The Head of IT must promptly review the details of all IT-related bills to ensure that the charges are appropriate, that no significant mistakes have been made, and that no significant unauthorized usage has occurred.

2.8.16 Prohibition Against Programs Consuming Excessive System Resources

Computer users must not run or write any computer program or process which is likely to consume significant system resources or otherwise interfere with MACRA's business activities.

2.8.17 Restricted And Monitored Use Of Systems Software Utilities

Access to systems software utilities must be restricted to a small number of trusted and authorized users. Whenever these utilities are executed, the resulting activity must be securely logged, and promptly thereafter reviewed by the Audit Division.

2.8.18 Tools Used To Break Systems Security Prohibited

Any software or hardware tools that can be used to break the security of the system is strictly prohibited unless authorized by the management for security testing purpose or fraud detection.

2.9 Hardware Controls

2.9.1 Hardware Procurement

The hardware procurement must be done in accordance with MACRA's procurement policy. Any hardware acquisition must be done within the yearly budget approved. Any procurement outside the projected budget must be approved by Management as per MACRA's policy.

2.9.2 Hardware Inventory

All computers, communication equipment, and other computer-systems-related hardware must be included in a comprehensive inventory system to monitor and account for its location, cost, movement, usage, and accountability. MACRA standard templates should be used.

Hardware and equipment must have up-to-date property tags to account for their existence during the physical inventory. The tag should include the serial number.

2.9.3 Use Of Computer Systems Belonging To Workers On Authority Property

Workers must not bring their own computers, peripherals, and other types of equipment into MACRA facilities without prior authorization from their department head.

2.9.4 Adequate Information Systems Insurance Coverage Must Be Maintained

Adequate insurance coverage must be obtained and kept in force for major threats facing the confidentiality, integrity, and availability of information handled by MACRA computer and communication systems.

2.10 Information Handling Controls

2.10.1 Handling of Third Party Confidential and Proprietary Information

Unless specified otherwise by contract, all confidential or proprietary information that has been entrusted to MACRA by a third party must be protected as though it was MACRA's confidential information.

2.10.2 Transfer Of MACRA's Information To Third Parties

MACRA software, documentation, and all other types of internal information must not be sold or otherwise transferred to any parties for any purposes other than business purposes expressly authorized by management.

2.10.3 Disclosure of Customer Personal Information

All customer records containing personal information that is in the possession of MACRA will be used only for purposes directly related to MACRA's business. Customer information will be disclosed to outside parties only with the customer's permission or if MACRA has received either a subpoena or a court order.

Information gathered about customers or potential customers, such as phone numbers and addresses, must only be used for internal MACRA purposes.

MACRA is serious about customer privacy. Its information systems do not employ secret serial numbers, secret personal identification numbers, or any other secret mechanisms which might reveal the identity or activities of customers.

2.10.4 Internet Use Of Other Organization's Trademarks and Service Marks

MACRA's web and commerce sites must not use any other organization's trademarks or service marks anywhere (text on pages, metatags, etc.) unless (a) the usage reflects the actual attributes of MACRA's products or services, and (b) advance permission has been obtained from MACRA's corporate legal counsel.

2.10.5 Third-Party Use Of MACRA’s Name

No third-party organization may use MACRA’s name in its advertising or marketing materials unless the permission of corporate legal counsel or its equivalent has first been obtained.

2.11 Information Storage And Disposal

2.11.1 Information Retention Period

Unless the type of information is specifically listed on the Information Retention Schedule, information must be retained for as long as necessary.

The information listed on the Information Retention Schedule must be retained for the period specified. Information in Hard Copy form must be destroyed when no longer needed—generally within five (5) years.

Information in electronic form must not be destroyed within the span of at least seven (7) years as required by the regulation of the Central MACRA of Malawi.

The retention of forms of backup or information must comply with local MACRA laws and regulations.

2.11.2 Regular Purging Of Information Which Is No Longer Needed

All MACRA information must be destroyed or disposed of properly and securely when no longer needed. To support this policy, management must review the continued value and usefulness of information on a periodic and scheduled basis.

2.11.3 Archival Of Information

All archival backup data stored offsite must be reflected in an up-to-date directory which shows the date when the information was most recently modified, as well as the nature of the information.

Sensitive, valuable, or critical information stored for periods longer than six months must not be stored on media subject to rapid degradation. For example, thermal fax paper or any document in thermal paper is not suitable for archival data storage media.

Critical business information and critical software archived on computer storage media for prolonged periods of time must be tested at least annually to ensure that the information is still recoverable.

The computer data media used for storing sensitive, critical or valuable information must be high quality and must be periodically tested to ensure that it can properly record the information in question. Used data media that can no longer reliably retain information must not be used for archival storage.

Computer media storage procedures must assure that sensitive, critical, or valuable information stored for prolonged periods of time is not lost due to deterioration. For instance, management must copy data to different storage media if the original backup media is showing signs of undue deterioration.

2.11.4 Procedure For Release Of Equipment Or Media To Third Party

Before any MACRA information systems equipment or storage media which has been used by MACRA is provided to any third party, the equipment or media must first be physically inspected by the IT Department to determine that all sensitive information has been removed.

2.11.5 Information Destruction and Information Systems Equipment Disposal

Department managers are responsible for recommending to the Administration Department the prompt and proper disposal of surplus property no longer needed for business activities. Disposal of information systems equipment must proceed in accordance with procedures established by the IT Department and/or Administration Department, including the irreversible removal of information and software.

Workers must not destroy or dispose of potentially important MACRA records or information without specific advance management approval. Unauthorized destruction or disposal of MACRA records or information will subject the perpetrator to disciplinary action including termination and prosecution. Records and information must be retained if: (1) they are likely to be needed in the future, (2) regulation or statute requires their retention, or (3) they are likely to be needed for investigation or prosecution of unauthorized, illegal, or abusive acts.

Workers must not destroy MACRA records unless these records (1) appear on a list of records authorized for destruction, and (2) can be destroyed according to instructions appearing in MACRA Records Retention and Disposition Schedule. Destruction is defined as any action which prevents the recovery of information from the storage medium on which it is recorded (including encryption, erasure, and disposal of the hardware needed to recover the information).

All financial accounting, tax accounting, and legal records must be retained for a period of at least ten (10) years or as required by the regulating bodies. All other records must be retained for a period of at least five (5) years or as required by the regulating bodies.

2.11.6 Disposal Of Sensitive Information

When disposed of, all secret, confidential, or private information in hardcopy or electronic form (paper, microfilm, microfiche, handwritten notes, CDs, tapes, files, etc.) must be either shredded or incinerated.

All MACRA offices and other areas where sensitive information is handled must have operational shredders. The people working in these areas must also be informed which materials need to be shredded.

Sensitive information must not be discarded in trash bins, recycle bins, or other publicly-accessible locations. Instead, this information must be placed in a designated locked destruction container within MACRA offices.

An exception is made in the case of secret information, which must be immediately destroyed by approved methods (shredding, burning, etc.)

Trash containing sensitive information that has been set aside for special destruction must be destroyed according to approved procedures regardless of recycling implications.

When no longer needed, all sensitive or valuable MACRA information must be securely destroyed using procedures approved by the management.

All materials used in the handling of sensitive information, which could be analyzed to deduce sensitive information, must be destroyed in a manner similar to that required for sensitive information. This policy covers typewriter ribbons, carbon papers, mimeograph stencil masters, photographic negatives, thermal fax transfer films, aborted computer hardcopy output, unacceptable photocopies, etc.

2.12 Backup And Disaster Recovery

2.12.1 Real-time Data Replication

MACRA shall at all times maintain an online real-time replication of data between the production systems and the disaster recovery systems.

2.12.2 Backup Control List

MACRA must maintain an up-to-date Backup Control List to identify data that needs to be backed up.

The Backup Control List must be prepared on a per department, unit, and branch basis.

The Backup Control List must clearly state the level of importance of the backup and its inclusion into the backup for disaster recovery.

2.12.3 What Data to Back Up And Minimum Backup Frequency

All critical business information and critical software resident on MACRA computer systems must be periodically backed-up. These backup processes must be performed as per the documented backup procedure of MACRA.

2.12.4 Periodic and Supplementary Backups Required For Portable Computers

Because theft of portable computers is so common, workers using these computers must make backups of all critical information prior to taking out-of-office trips. These backups should be stored elsewhere than the portable computer's carrying case. This precaution supplements the periodic backup that must otherwise be made.

A documented backup procedure for laptops must exist for each MACRA.

2.12.5 Initial Backup Copies Of Software

All software must be copied prior to its initial usage and original or master copies must be stored in a safe and secure location.

These duplicate copies must be used for the recovery from computer virus infections, hard disk crashes, and other computer problems.

Ghost images must be used to back up the configuration of each computer.

2.12.6 Use Of Labels To Backup Disk And Other Storage Media

Labels should be used for every backup disk, tape, or other storage media, detailing information backed up and date.

If information is either secret, confidential, or private, all instances in which it is displayed on a screen or otherwise presented to a computer user must include an indication of the information's sensitivity.

2.12.7 Two Copies Of Sensitive, Critical, Or Valuable Information

Unless other backup arrangements are known to be operational, all users are responsible for making available to the IT Department the documents they want to back up. These separate backup copies should be made as per the backup policy of MACRA.

At least one recent and complete backup (not incremental backups) made on different dates containing critical MACRA records must always be stored off-site.

2.12.8 Monthly Archival Backups Required For All Critical Information

Critical business information and critical software must be backed up onto archival storage media and kept for at least a year. These backups must be made as per the backup policy of MACRA.

2.12.9 Off-Site Storage Of Backup Media

Backups of essential business information and software must be stored in an environmentally-protected and access-controlled site that is a sufficient distance away, or as dictated by the written contingency plan, from the originating facility to escape a local disaster.

One copy of the offsite backup media must be stored in the Offsite backup system facility.

Backup media contents stored off-site must be encrypted or password protected.

Backup media encryption keys and passwords must be kept in a vault or other location identified by the management as secure, such as a Safe Deposit Box (SDB). Other copies of these encryption keys and passwords must be stored in the Offsite backup system facility.

2.12.10 Access Control For User File Restoration Process

Users must not be given the ability to restore their own files. All restoration processes must be performed by an authorized system administrator.

2.12.11 Make At Least One Copy Of Critical Backed-Up Files Prior To Use

Critical data which has been backed up must not be used for data restoration purposes unless another backup copy of the same data exists on different computer storage media (tape, disk, smart card, CD-ROM, etc.).

If a computer virus or other software problems are suspected, the additional backup copy should be made on a different computer.

This policy will prevent the only current copy of critical backup data from being inadvertently damaged in the process of restoration.

2.12.12 Regular Review Of Backup Data Through Auditing Procedures

All backups as specified in the Backup Control List in all departments, units, and branches must be included in regular compliance or auditing procedures performed by MACRA's Audit Department.

2.12.13 Off-Site Backup Systems

MACRA must create and maintain offsite Backup Systems, including applications, ready to run as production systems in the event of a disaster.

Offsite Backup Systems must be protected and controlled in terms of access, theft, public viewing, and other activities that may be harmful to the systems.

The offsite backup systems must be located at least 10 kilometers away from the location of the production systems and not located in the Central Business District (CBD) and/or Financial district of the towns or cities where the production systems are located.

The offsite backup systems must contain up-to-date information from the production systems.

Offsite backup systems must adhere to the existing Regulating Bodies' specifications and requirements.

The responsibility of the custodians to the offsite backup system must be defined, documented, understood, and contractually signed by the appointed custodians.

Offsite backup systems must be checked and updated as the production systems are updated once every 3 months, or as needed to ensure reliability and successful recovery in the event of a disaster.

2.12.14 Disaster Recovery Procedures

MACRA must develop comprehensive and functional disaster recovery procedures aligned to the offsite backup systems setup, contingency plans, and existing policies and procedures.

Documents pertaining to Disaster Recovery procedures must be kept in a secured place outside the building where the production systems are located. Another copy must be available in the offsite backup systems location.

Documents related to Disaster Recovery must be updated whenever the production systems itself and its documentation is updated.

Disaster Recovery procedures must be tested once a year to ensure reliability and successful recovery.

2.12.15 Users Documents

MACRA shall use a combination of cloud-based storage and on-premises file server-based solutions to store business-related documents for all users. Users with Microsoft Office 365 accounts will use Microsoft OneDrive to store all business-related information and secure and private folders will be configured on the server and mapped on users' profiles for users without Microsoft Office 365 accounts. ICT depart must configure both OneDrive and mapped drives for all user's profiles on their primary computer.

Users shall have the responsibility to store business-related files on either Microsoft Office OneDrive or file servers.

2.13 Personnel Controls

2.13.1 Confidentiality Agreement Required For All MACRA Workers

All employees and contractors (temporaries, consultants, outsourcing firms, etc.) must personally sign a MACRA non-disclosure agreement or confidentiality statement. The provision of a signature must take place before work begins, or if a worker has been working without a non-disclosure agreement, a signature must be provided as a condition of continued employment.

2.13.2 Background Checks for Computer-Related Positions Of Trust

All workers to be placed in computer-related positions of trust must first pass a background check. This process shall include examination of criminal conviction records and lawsuit records as well as previous employment. This policy applies to new employees, re-hired employees, and seconded employees, as well as third parties like temporaries, contractors, and consultants.

2.13.3 IT Staff Roles and Responsibilities

All IT Staff must have clear job descriptions with tasks, roles, responsibilities, and outputs. Each worker must have daily/weekly/monthly/yearly checklists to follow.

2.13.4 Technical Information Systems Staff Seminars and Training

All technical information systems staff must have sufficient initial training as well as continuing education in all critical aspects of their jobs including security, quality assurance, technical supports, and customer relations. The Head of IT in collaboration with the HR Head is responsible for providing the necessary training.

2.13.5 Information Security Considered In Employee Performance Evaluations

Compliance with the information security policies and procedures must be considered in all employee performance evaluations.

2.13.6 Avoid Actual And Apparent Conflict Of Interest

All workers must avoid the actual or apparent conflict of interest in their business-related dealings with MACRA. Should there be any doubt as to the existence of a potential conflict of interest the worker must consult his or her Department manager.

2.13.7 Information Must Not Be Shared With Competitors

In any social, familial, or other contact with employees of competing organizations, MACRA staff must be careful not to divulge information, directly or indirectly, which might lead to loss of advantage or another compromise.

2.13.8 Notification And Handling Of Employees Leaving For Competitor

All workers intending to work for a competitor must immediately notify MACRA management at the time they accept the offer to work for the competitor. All the rights, privileges, and accesses which have been extended to such a worker may be immediately revoked at the management's discretion.

2.13.9 Handling Involuntary Terminations Of IT Department Workers

In all cases where IT support workers are involuntarily terminated, they must be immediately relieved of all of their duties, required to return all MACRA's equipment and information, and escorted while packing their belongings and walking out of MACRA facilities.

2.13.10 Removal Of Information Upon Termination Of Employment

Upon termination of employment, workers may not retain, give away or remove from MACRA's premises any of MACRA information other than personal copies of information disseminated to the public and personal copies of correspondence directly related to the terms and conditions of their employment. All other MACRA information in the custody of the departing worker must be provided to the worker's immediate supervisor at the time of departure.

2.13.11 Return of Information By Contractors, Consultants, And Temporaries

Upon the termination or expiration of their contract, all contractors, consultants, and temporary employees must hand over to the project manager all copies of MACRA information received or created during the performance of the contract.

2.13.12 Return Of MACRA's Property At The Time Of Separation From MACRA

When employees, consultants, and contractors terminate their relationship with MACRA, all MACRA's property must be returned. This includes portable computers, library books, documentation, building keys, magnetic access cards, credit cards, outstanding financial obligations, and the like.

These terminating individuals must inform management about all MACRA's property they possess, as well as all computer system privileges, building access privileges, and other privileges that they have been granted.

2.13.13 Responsibility for Taking Action In Response To Worker Termination

When an employee, consultant or contractor terminates his or her relationship with MACRA, the worker's immediate manager or supervisor is responsible for:

- Ensuring all property in the custody of the worker is returned before the worker leaves MACRA.
- Notifying all administrators handling the computer and communications accounts used by the worker as soon as the termination is known.
- Terminating all other work-related privileges of the worker at the time that the termination takes place.
- Notifying all concerned parties (HR, Operations, Finance) about his/her outstanding obligations.

2.13.14 Transfer Of Information Custodian Duties After Employee Terminations

When a worker leaves any position with MACRA, both computer-resident files and paper files must be promptly reviewed by his or her immediate manager to determine who should become the custodian of such files, and/or the appropriate methods to be used for the file disposal. The computer user's manager must then promptly reassign the computer user's duties as well as specifically delegate responsibility for the files formerly in the computer user's possession.

2.13.15 Schedule For Deletion Of Files Following Worker Termination

When the IT department has received instructions from the HR department, four weeks after a worker has permanently left MACRA, all files held in the user's directories will be purged, with the authorization of the worker's supervisor.

2.13.16 Reliance On Single Person For Important Systems Expertise

Expertise in important computer or communications-related areas must be possessed by at least two available persons. Having such backup expertise prevents undue interruptions in systems service, and also increases the likelihood that unauthorized and abusive acts will be noticed.

2.13.17 Loss Of Critical Knowledge And Key Employees Taking Same Means Of Transport

To protect MACRA's pool of knowledge and skills, it is advised that employees with critical knowledge from the same department do not take the same vehicle or flight.

2.13.18 Drug-Free and Alcohol-Free Work Place

Except for prescriptions ordered by licensed health care professionals, workers must not be impaired by either drugs or alcohol when at the workplace.

2.13.19 Sensitive Information Access for Employees, Temporaries, And Consultants

Activities requiring access to sensitive MACRA information must only be performed by full-time permanent employees unless one of the following conditions prevail:

- The requisite knowledge or skills are not possessed by a full-time permanent employee.
- An emergency or disaster requires the use of additional workers.
- Permission from the Head of the Human Resources Division has been obtained.

2.13.20 Disciplinary Measures for Information Security Non-Compliance

Non-compliance with information security policies, standards, or procedures is grounds for disciplinary action up to and including termination.

2.13.21 Disciplinary Measures for Various Information Security Violations

Assuming the violation is inadvertent or accidental, first violations of the information security policies or procedures must result in a warning. Second violations involving the same matter must result in a letter being placed in the involved worker's personal file. Third violations involving the same matter must result in a five-day suspension without pay. Fourth violations involving the same matter must result in dismissal. Wilful or intentional violations, regardless of the number of violations, may result in disciplinary action up to and including immediate dismissal.

2.13.22 Security Violations Requiring Instant Terminations

All workers who have stolen MACRA property, acted with insubordination, or been convicted of a felony, must be dealt with in accordance with MACRA's HR policy and the country's legislation.

2.13.23 Prohibition against Sexual, Ethnic, and Racial Harassment

Sexual, ethnic, and racial harassment—including telephone calls, electronic mail, and internal mail—is strictly prohibited and is cause for disciplinary action including termination. Managers must make this policy clear to workers in their group and must promptly investigate and rectify any alleged occurrences.

2.14 Physical and Environmental Protection

2.14.1 ID Cards Must Be Worn In Visible Place When In MACRA's Premises

All persons must wear identification cards on their outer garments so that both the picture and information on the ID card are clearly visible whenever they are in MACRA buildings or facilities.

2.14.2 Temporary IDs for Visitors and Workers Who Have Forgotten Their IDs

Visitors and workers who have forgotten their identification cards must obtain a temporary ID card by presenting valid identification documents. A temporary ID card is valid for a single day only.

All visitors must show valid identification documents with picture and signature and be issued with a visitor temporary ID card prior to gaining access to restricted areas controlled by MACRA. Visitors must be admitted to MACRA only for a specific and legitimate purpose.

2.14.3 Reporting Lost/Stolen IDs And System Access Cards/Tokens

Identification cards and physical access cards that have been lost or stolen—or are suspected of being lost or stolen—must be reported to the HR department immediately.

All computer or communication system access tokens (smart cards with dynamic passwords, telephone credit cards, etc.) that have been lost or stolen—or are suspected of being lost or stolen—must be reported to the Administration and IT departments.

2.14.4 Physical Access Control For Areas Containing Sensitive Information

Access to every office, computer room, and work area classified as a restricted area or containing sensitive information must be physically restricted.

2.14.5 When Offices Are Not In Use, The Doors Must Be Locked

All workers with separate personal offices must lock the doors when these offices are not in use. Although other measures will also be necessary, this practice will help to restrict unauthorized access to sensitive information.

2.14.6 Location Of Data Processing, Data Storage, And Host Servers Are Restricted Areas

Information about the nature and location of MACRA information, such as that found in a data dictionary, is confidential and must only be disclosed to those who have a demonstrable need-to-know.

The data center's physical location is confidential and must not be disclosed to those without demonstrable need-to-know.

The data center or main storage area must not be labelled, to hide its location from visitors.

2.14.7 Multi-User Computers, Servers, And Communication Systems In Locked Rooms

All multi-user computer and communications equipment must be located in a locked room or security-system controlled room to prevent tampering and unauthorized usage.

2.14.8 Centralization Of All Critical Voice And Data Networking Devices

All business-critical devices supporting MACRA telephone system, intranet, local area networks, and the wide-area network must be centralized in dedicated rooms (data centers) with physical access controls, close circuit TV (when necessary), environmental monitoring systems, and other security measures.

2.14.9 Data Center Is a Closed Shop

MACRA's data centers are closed shops. Programmers, users, and others without a business need for such access are not permitted inside the data center.

2.14.10 Workers Must Not Take Any Luggage into Restricted Areas

Luggage must not be allowed in restricted areas. Luggage should be left at the reception area or in any place wherein luggage deposit is officially designated by the management.

2.14.11 Vacated Equipment Areas Must Be Locked And Periodically Checked

All vacant information systems equipment areas must be locked and periodically checked by either remote monitoring systems and/or a security guard.

2.14.12 Changing Access Control Codes On Worker Termination

When a worker terminates his or her working relationship with MACRA, all physical security access codes known by the worker must be deactivated or changed. For example, the password entered on a computer-controlled entrance door to get into the building must be changed.

2.14.13 Escorts Required For All Visitors

Visitors to MACRA offices must be always escorted by an authorized employee, consultant, or contractor. This means that an escort is required as soon as a visitor enters a controlled area and until this same visitor goes outside the controlled area. Visitors requiring an escort include customers, package delivery Authority staff, other authorities ’ messengers, and police officers.

2.14.14 Third-Party Supervision In Areas Containing Sensitive Information

Individuals who are neither MACRA employees, nor authorized contractors, nor authorized consultants, must be supervised whenever they are in restricted areas containing sensitive information.

2.14.15 Public Tours Of Computer Facilities Prohibited

Public tours of major computer and communications facilities are prohibited unless authorized by the senior management.

2.14.16 Positioning Of Computer Display Screens With Respect To Windows

The display screens for all PCs, workstations and dumb terminals used to handle sensitive or valuable data must be positioned so that they cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related public areas.

2.14.17 Cameras Plus Audio And Video Recording Equipment Prohibited

Within the controlled perimeters of MACRA offices, cameras and audio or video recording equipment is not allowed, unless authorized by the management.

2.14.18 Areas Where Electronic Monitoring Of Workers May Be Used

Workers may be subject to electronic monitoring while on MACRA's premises. This monitoring is used to measure workers' performance as well as to protect workers' personal property, workers' safety, and MACRA's property.

In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms, and locker rooms, no electronic monitoring will be performed.

2.14.19 Location Of New Data Centers

As far as practically possible, all new MACRA data centers must not be located in an area likely to experience a natural disaster, serious man-made accidents (chemical spills, the dangerous release of nuclear materials, etc.), riots, and related problems.

2.14.20 Adequate Data Centers

New and remodeled MACRA data centers must be constructed so that they are protected against fire, water damage, vandalism, and other threats known to occur, or that are likely to occur at the involved locations.

To minimize theft and water damage, multi-user computers and communications facilities must be located above the first floor in buildings, where possible. To minimize potential damage from smoke and fire, kitchen facilities should be located away from (including not directly above or below) multi-user systems. Likewise, to minimize potential water damage, restroom facilities should not be located above these systems. To minimize unauthorized electromagnetic eavesdropping and interference, these systems should not be located adjacent to a building's exterior wall.

2.14.21 Data Center Fire Extinguisher Installed

Approved fire extinguisher and dry chemical fire control devices must be installed within the data center.

2.14.22 Data Centers And Automatically Closing Doors

Ideally, data rooms should be equipped with doors that automatically close immediately after they have been opened, and which set off an audible alarm when they have been kept open beyond a certain period of time.

2.14.23 Fire And Physical Intrusions Alarms Trigger Immediate Action

MACRA's data centers must be equipped with fire, water, and physical intrusion alarm systems that automatically alert those who can take immediate action.

2.14.24 Devices Prone To Create Explosion, Shortage, And Fire Prohibited

Repairs, soldering, welding, and other activities that might create an explosion, electrical shortage, heat, or fire must not be performed inside the data center.

Radios, cellular phones, and other communication devices prone to explosion must not be carried inside the data center, including for recharging of such devices.

Any equipment or devices with the potential to create an explosion, fire, or any form of damage must not be taken inside the data center.

A fire extinguisher must exist in areas where repairs, soldering, or welding are carried out.

2.14.25 Computing Environment Supporting Equipment Required

Local management must provide and adequately maintain fire detection/suppression, power conditioning, air conditioning, humidity control, dust control, air purifier (when necessary), or other computing environment protection systems necessary to assure continued service for critical production computer systems.

All PCs and workstations must be outfitted with uninterruptible power supply (UPS) systems, electrical power filters, or surge suppressors which have been approved by the Head of IT and are in accordance with MACRA standards.

If weather and building conditions pose a significant risk of static electricity discharge, all PCs and workstations must be outfitted with static protection equipment which has been approved by the Head of IT. This will ensure that the discharge of static electricity does not damage computer equipment or information.

Power generators and UPSs may be used to run critical production computer systems in the event of a power failure.

Critical online production systems must have a backup communication system installed, for use in the event of failure of the primary communication system.

2.14.26 Smoking, Eating And Drinking Close To The Computer Machines

Workers and visitors must not smoke, eat, or drink next to the computer machines or other IT equipment. To do so would risk damage to equipment as well as risk particulate contamination to data storage devices.

2.14.27 Air Conditioning Machines

Ideally, air conditioners must not be placed above any computer equipment.

2.14.28 Equipment Maintenance

The Head of IT is responsible for periodic equipment maintenance (including for servers, computers, air conditioners, power equipment, telecom and network equipment, copiers, printers, fax machines, scanners, PABX, etc). This can be achieved through internal processes or contract with external service providers.

2.14.29 Storage Media Protection

All storage media (CDs, tapes, etc) must be stored in an appropriate location to protect them from damage and information loss.

2.14.30 Emergency Procedures Training

All workers must be trained in emergency procedures.

2.14.31 Computer And Communication Equipment Tracking Stickers

Every item of MACRA's computer and communications equipment must have a unique identifier (ideally computer-readable) attached to it such that physical inventories can be efficiently and regularly conducted.

Every item of MACRA's computer and communications equipment must have an identification number permanently etched onto the equipment. This code will assist police in their attempts to return the property to its rightful owner.

2.14.32 Moving Microcomputer Equipment without Approval Prohibited

MACRA's computer and communications equipment, including storage media, must not be moved or relocated, within or outside MACRA's premises, without the prior approval of the Head of IT.

An exception will be provided for equipment for which a move approval form has been obtained (mobile computing equipment, telecommuter equipment, etc.)

2.14.33 MACRA's Devices Not To Be Lent To Others

Workers must not lend to others any personal computers, handheld computers, transportable computers, smartphones, or any other devices used for business activities if the machine contains sensitive information.

2.15 Contingency Plans

2.15.1 Framework For Segmenting Information Resources By Recovery Priority

The management must establish and use a logical framework for segmenting information resources by recovery priority. This will in turn allow the most critical information resources to be recovered first. The IT Department and other departments must use this framework when preparing information systems contingency plans.

2.15.2 Annual Criticality Rating For Multi-User Applications

In conjunction with relevant information owners, the IT Department must periodically prepare or revise an assessment of the degree of criticality of all production multi-user computer applications. This rating process will allow appropriate contingency plans to be prepared.

2.15.3 Five Category Application Criticality Classification Scheme

All production computer applications must be placed into one of five criticality classifications, each with separate handling requirements: highly critical, critical, priority, required, and deferred. This criticality classification system must be used throughout MACRA and must form an integral part of the system contingency planning process.

2.15.4 Preparation And Maintenance Of Computer Emergency Response Plans

For computer and communications systems, management must prepare, periodically update, and regularly test emergency response plans. These plans must provide for the continued operation of critical systems in the event of interruption or degradation of service.

2.15.5 Inventory Of Key Technical Jobs And Individuals Who Fill Them

Management must annually prepare an inventory of key MACRA technical jobs and the names of the individuals who currently fill these jobs.

2.15.6 Cross Training For Staff In Critical Technical Jobs

At all times, at least two staff members should be able to provide essential technical services for information systems critical to MACRA business. If fewer than two staff members can provide these essential technical services, management must initiate cross-training, additional hiring, outsourcing, or other remedial actions.

2.15.7 Preparation And Maintenance Of Computer Disaster Recovery Plans

Management must prepare, periodically update, and regularly test a disaster recovery plan that will allow all critical computer communication systems to be available in the event of a major loss such as a flood, earthquake, or cyclone.

2.15.8 Annual Inventory Of Information Systems Hardware, Software Etc.

So that the current computing environment may be quickly re-established following a disaster, the IT Department must prepare an annual inventory of production information systems. This inventory must indicate all existing production information systems, production hardware, software, and communication links.

2.15.9 Annual Determination Level Of Disaster/Emergency Support Levels

Management must agree on the support levels that will be provided in the event of a disaster and/or emergency. These levels must appear in contingency planning documents or service agreements.

2.15.10 Computer And Communications System Contingency Plan Testing

Computer and communication system contingency plans must be tested at regular intervals to assure that they are still relevant and effective. Each test must be followed by a brief report to top management detailing the results of the test and any remedial actions that will be taken.

2.15.11 Preventive And Comprehensive Maintenance On Computer And Communication Systems

Preventive maintenance must be regularly performed on all computer and communications systems so that risk of failure is kept to a reasonably low probability.

All information systems equipment used for production processing must be maintained in accordance with the supplier's recommendation service intervals and specifications. Repairs and servicing of equipment must be performed only by qualified and authorized maintenance personnel.

2.15.12 Contact Numbers For Information Technology Staff And Key Officers Of MACRA

All key officers of MACRA must provide the management with complete contact details including mobile phones, and other means of contacting them.

2.15.13 Safekeeping Of Backup System Keys, Key Cards, And System Access Codes

Backup system keys, key cards, system access codes, and passwords must be kept a sufficient distance from the main building. These backup system keys and codes must be stored in a safety deposit box in a branch or other MACRA outside the premises.

2.15.14 Required Action Following Suspected System Intrusion

Whenever a systems administrator has good reason to believe that an information security system has been compromised, a file comparison utility must be run on the system involved to identify all changes to systems software, and the systems software environment must be restored from trusted backup copies.

Before being reconnected to the network, the access control systems must be reinitialized (for example all fixed passwords must be changed).

The current system log must be copied to separate data storage media which is then kept in a locked container.

2.15.15 Regular Monitoring Of Information Security Vulnerability Advisories

On a weekly or more frequent basis, the systems administrator must review all information security vulnerability advisories issued by trusted organizations or government agencies and other direct implementing bodies.

2.16 Change Management Controls

2.16.1 Change Control Procedure For Production Systems

All computer and communication systems used for production processing at MACRA must employ a formal change control procedure which is used to ensure that only authorized changes are made. This change control procedure must be used for all significant changes to software, hardware, communication networks, and related procedures.

The procedure that will be followed for any change that is to be made to systems is as follows:

- An appropriate Work Request Form (WRF) must be completed by the business user who is requesting the change.
- The completed WRF must be authorized by the head of the department from the requesting user's department.
- The authorized WRF must be approved by a member of MACRA's ExCO.
- The approved WRF must be handed over to the Head of the ICT Department to initiate the necessary work to meet the requested business requirement.
- Development work for the requested business requirement must be done in a test environment. On completion of development, Services Delivery Manager from ICT Department will inform the user who requested the change to test.
- The user will perform User Acceptance Testing (UAT) on the provided test environment using Test Scripts and/or Test Data.

- On successful completion of UAT, the user will sign off the Test Scripts and these will be made available to the Services Delivery Manager from ICT Department.
- On receipt of the signed-off Test Scripts, a form will be completed within ICT Department to request the change to be implemented on a production system. On this form, details of the ICT officer who is requesting to deploy the new system development to production; details of the change; details of the ICT Manager who checked the change; approval by the Head of ICT Department to have the change effected on a production system; details of the ICT officer who is to deploy the change in the production system.
- An appropriate roll-back procedure must be followed when problems occur during or after change implementation with data backups being taken prior to and after the change has been implemented in the system.

2.16.2 User Acceptance Testing (UAT) Requirements

Users Acceptance Testing (UAT) with Test Scripts and/or Test Data is required at all times in the following situations:

- Before the implementation of any newly developed system
- Before any changes to the production system

The users' certification or sign-off documents are required when the UAT is completed. This is for the users to accept that the UAT process is complete and all the test results meet the users' requirements.

2.17 Integrity Controls

2.17.1 Acceptable Risk Of Undetected Information Alteration

Management must establish and maintain sufficient preventive and detective security measures to ensure that MACRA information is free from significant risk of undetected alteration.

2.17.2 Authorization For Changes To Production Data And Programs

MACRA production data and production computer programs must be changed only by authorized people according to established procedures.

2.17.3 All Production Transactions Must Be Authorized And Verified By Management

Transactions that update business records must only be processed if they have first been authorized by MACRA management.

Management must review (or establish mechanisms for suitably qualified and responsible people to review) the reasonableness and accuracy of all changes to internal records. These changes include posting of transactions, recording receipts, and disbursements, etc.

2.17.4 Standard Control Procedures For Correcting Business Records

If MACRA business records are shown to be in error, they must be promptly corrected using the standard control procedures.

The control procedures or correcting processes must be clearly documented.

2.17.5 Data Conversion

Before any data is converted from one system to another as a result of cases such as but not limited to system upgrades and system changes, there shall be a data conversion strategy that will be required to be produced and approved before any data is converted.

The conversion may require processing by the use of a special conversion program, or it may involve a complex process of going through intermediary stages, or involving complex "exporting" and "importing" procedures, which may include converting to and from a tab-delimited or comma-separated text file. In some cases, a program may recognize several data file formats at the data input stage and then is also capable of storing the output data in a number of different formats. Such a program may be used to convert a file format.

The data conversion strategy shall cover all such areas including tools that will be used as well as processes that will be followed.

2.17.6 Data Corruption Verification

The IT department must periodically verify the systems for any data corruption. This can be done using existing tools.

2.17.7 Downloading Of Data

Before any secret, confidential, or private information is transferred from one computer to another, the person making the transfer must make sure that access controls on the destination computer are at least as secure as access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred.

Sensitive MACRA information may be downloaded from a multi-user system to a PC or a workstation only if (1) a clear business need exists, and (2) advance permission from the information owner is obtained. This policy is not intended to cover electronic mail or memos but does apply to databases, master files, and other information stored on mainframes, minicomputers, servers, and other multi-user machines.

Systems that automatically exchange data between devices, such as a portable cellular telephone, personal computer, or other devices, must not be used unless the systems have first been evaluated and approved by the management.

2.17.8 Dealing With Malicious Software

Malicious software includes viruses, trojans, rootkits, spyware, etc. Malicious software can spread quickly via data storage media (floppy disk, magnetic tapes, etc.) and/or across networks. It must be eradicated as soon as possible to limit serious damage to computers and data.

Because malicious software has become very complex, users must not attempt to eradicate it without expert assistance. If users suspect infection by malicious software, they SHOULD NOT shut down the involved computer, but immediately disconnect from all networks, close all the applications and call MACRA help desk (or its equivalent). The IT Department must investigate immediately.

Users must not attempt to eradicate malicious software from their systems unless they are following the instructions of a system administrator or equivalent. This will help minimize damage to data files and software, as well as ensure that information needed to detect a re-infection has been recorded.

If malicious software is not promptly reported, and if the investigation reveals that certain workers were aware of the incident, those workers will be subject to disciplinary action which may include termination.

The IT Department must make sure the users are trained to identify malicious software and on immediate actions they must take.

2.17.9 Testing For Malicious Software Prior To Use On MACRA Systems

To prevent infection by malicious software, workers must not use any externally-provided software from a person or organization other than a known and trusted supplier. The only exception to this is when such software has first been tested and approved by the IT Dept.

2.17.10 Testing For Malicious Software On Non-Production Machine

Whenever software and/or files are received from any external entity, this material must be tested for unauthorized software on a stand-alone non-production machine before it is used on MACRA information systems. If a virus, worm, Trojan, or other malicious software is present the damage will be restricted to the stand-alone machine.

2.17.11 Prohibition Against Downloading Software From Third-Party Systems

Workers must not download software from electronic bulletin boards systems, the internet, external storage media or any other systems outside MACRA. This prohibition is necessary because such software may contain viruses, worms, Trojans, and other malicious software which may damage MACRA information systems.

2.17.12 Virus Checking At Firewalls, Servers, And Desktop Machines

Virus scanning software must be installed and enabled on MACRA’s firewalls, FTP servers, mail servers, intranet/internet servers, another type of server, and desktop machines.

Externally-supplied storage media may not be used on any of MACRA’s personal computers (PCs) or servers unless the media have been checked for malicious software and approved by the IT department.

To promptly detect and prevent the spread of malicious software, all MACRA personal computers (PCs) and servers must run integrity-checking software. This software detects changes in configuration files, system software files, application software files, and other system resources. Integrity checking software must be continuously enabled or run daily.

Virus scanning software must be continuously enabled on all local area network (LAN) servers and networked personal computers (PCs).

2.17.13 Assignment Of Patent, Copyright, And Other Intellectual Property Rights

While employed by MACRA, all staff members grant to MACRA exclusive rights to patents, copyright, inventions, or other related intellectual property they originate and/or develop.

Except for specific written exceptions, all programs and documentation generated by, or provided by employees, consultants, or contractors for the benefit of MACRA are the property of MACRA. Management must ensure that all workers providing such programs or documentation sign a statement to this effect prior to the provision of these materials.

2.17.14 Legal Ownership Of Information Systems Files And Messages

MACRA has legal ownership of the contents of all files stored in its computer and network systems. MACRA reserves the right to access this information without prior notice whenever there is a genuine business need.

2.18 Documentation Controls

2.18.1 Documentation Required For All Production Business Systems

Every user who develops or implements software and/or hardware to be used for MACRA business activities must document the system in advance of its development. The documentation must be written so that the system may be run by persons unacquainted with it. Such documentation must be prepared even when standard software—such as a spreadsheet program—is employed. Documentation must cover both business and technical references.

2.18.2 When To Prepare Production Systems Change Documentation

Documentation reflecting all significant changes to production computer and communications systems at MACRA must be prepared within the week from the time that a change took place. This documentation must reflect the proposed change, management approval, and the way in which the change was performed.

2.18.3 Training And Operating Documentation Required For Production Systems

Business application systems in development or undergoing significant modification must not be moved into a production processing environment without first having adequate training materials and operating documentation. The adequacy of these materials must be determined by the User Acceptance Test (UAT) team.

2.18.4 Release Of Systems Documentation To Third Parties

Prior to being released to third parties, all documentation that describes MACRA systems or systems procedures must be reviewed by the Management to ensure that confidential information is not being inadvertently disclosed.

2.19 Security Awareness and Training

2.19.1 Information Security Training Required

All workers (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect MACRA information resources.

2.19.2 IT Department Responsible For Information Security Training

The IT department must provide refresher courses and other materials to regularly remind all workers (employees, temporaries, consultants, contractors, etc) about their obligations with respect to information security.

2.19.3 Attendance At Information Security Seminar Mandatory

Every worker must attend an information security awareness seminar before they begin employment with MACRA. To provide evidence that every employee has attended the seminar, each employee must sign a statement that they have attended the seminar, understood the material presented and had an opportunity to ask questions.

2.19.4 Required User Training For Production Systems

MACRA’s workers must not use any software for production business processes unless they have first completed approved training for such software.

2.20 Electronic Mail (Email) Controls

2.20.1 Electronic Mail Account Must Be Protected With Password

Every electronic mail account must be protected from anyone who is not an owner. A password should be enforced by the owner upon the creation of his or her email account. When this password is made known to anyone except the owner, this should be changed immediately. If the owner forgets the password, the correct procedure for resetting the password must be followed.

2.20.2 Using An Electronic Mail Account Assigned To Another Individual

Workers must not use electronic mail account assigned to another individual to either send or receive messages. If there is a need to read another's mail (while they are away on vacation for instance), automatic message forwarding and other electronic facilities must instead be used.

2.20.3 Privacy Expectations And Electronic Mail

Workers must treat electronic mail messages and files as private information. Electronic mail must be handled as private and direct communication between a sender and a recipient.

2.20.4 Treat Electronic Mail As Public Communications

Workers should consider electronic mail to be the electronic equivalent of a postcard. Unless the material is encrypted, users must refrain from sending credit card information, password, research and development information, and other sensitive data via electronic mail.

2.20.5 Authorization To Read Electronic Mail Messages Of Other Workers

When the Head of IT and the Head of Human Resources agree to it, electronic mail messages flowing through MACRA systems may be monitored for internal policy compliance, suspected criminal activity, and other systems management reasons.

Unless electronic mail monitoring tasks have been specifically delegated by the above-mentioned managers, all workers must refrain from this activity.

2.20.6 Monitoring Of Electronic Mail Messages

Messages sent over MACRA's internal electronic mail systems are subject to monitoring and therefore may be read by MACRA management and system administrator.

2.20.7 Notification Of Content Monitoring For Electronic Mail Transmission

MACRA routinely employs automatic electronic mail content scanning tools to identify selected keywords, file types, and other information. Users should restrict their communications to business matters in recognition of this electronic monitoring.

MACRA prohibits large, attached files (music, video clips, images, etc.) in the electronic mail systems. Automatic barring of large, attached files must be installed or activated in the system to return back to sender all email messages with unacceptable attached files.

2.20.8 Users Must Not Employ Electronic Mail Systems As A Database

Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files. Electronic mail systems are not intended for archival storage of important information. Stored electronic mail messages may be periodically expunged by systems administrators, mistakenly erased by users, and otherwise lost when system problems occur.

2.20.9 Recording And Retention Of Electronic Mail

MACRA systems administrators must establish and maintain a systematic process for the recording, retention, and destruction of electronic mail messages and audit logs.

Such destruction must be postponed if the material might be needed for imminent legal action.

If an electronic mail message contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value as evidence of MACRA management decision, it should be retained for future reference. Most electronic mail messages will not fall into these categories, and so can be erased after receipt.

2.20.10 Periodic Destruction Of Archived Electronic Mail Messages

While management encourages periodic backups of computer-resident data, internal correspondence must be disposed of when no longer needed. To this end, all multi-user electronic mail logs must be destroyed one year after being archived. Electronic mail messages relevant to current activities, or that are expected to become relevant to current activities, should be saved as separate files and retained as long as needed.

2.20.11 Electronic Mail Messages Are Authority Records

MACRA electronic mail system is to be used only for business purposes. All messages sent by electronic mail are MACRA records. MACRA reserves the right to access and disclose all messages sent over its electronic mail system, for any purpose.

Supervisors may review the electronic mail communications of workers they supervise to determine whether they have breached security, violate MACRA policy, or take other unauthorized actions.

MACRA may also disclose electronic mail to law enforcement officials without prior notice to the workers who may send or receive such messages.

2.20.12 All Electronic Mail Archived And Subject To Supervisory Review

All electronic mail sent through the MACRA mail server is archived and subject to review by people other than the recipient and sender.

2.20.13 Forwarding Copies Of Official Electronic Mail To Archival Records

All official MACRA electronic mail messages, including those containing a formal management approval, authorization, delegation, or handing over the responsibility, or similar transaction, must be copied to the Administration Office or as designated by the management.

2.20.14 Common Electronic Mail Program Must Be Used

Common applications for reading electronic mail must be used by each worker of MACRA. This is to make use of common technical support, avoid contamination by malicious software, and avoid legal problems with regard to the use of unlicensed software. If the exemption is required, management approval must be obtained.

2.20.15 Personal Use Of Electronic Mail Systems

Electronic mail systems are intended to be used primarily for business purposes. Any personal use must not interfere with normal business activities, must not involve solicitation, must not be associated with any for-profit outside the business activity, and must not potentially embarrass MACRA.

Personal use of MACRA’s email system should not violate the policy on privacy or secrecy of information and other policies of MACRA.

Personal use of MACRA’s email system must be minimal.

Personal use of MACRA’s email system must not involve criminal acts, terrorism, or other activities against the law of the land.

2.20.16 Authorization To Issue Broadcast On Electronic Mail

Broadcast facilities found in electronic mail systems and voice mail systems may only be used by department heads or upper management of MACRA.

2.20.17 Sender Contact Information Must Be Included In Electronic Mail

To facilitate communications and to properly identify the sending party, all electronic mail sent using MACRA information systems must contain the sender’s first and last name, job title, organizational unit, and telephone number. This should be done in the signature of each user.

2.20.18 Misrepresentation Of Identity On Electronic Mail System

Users’ identities on electronic communications must not be misrepresented, obscured, suppressed, or replaced. The username, electronic mail address, organizational affiliation, and related information included with message or postings must reflect the actual originator of the message or postings.

2.20.19 Prohibition Against Use Of Scanned Hand-Rendered Signatures

Workers must not employ scanned versions of hand-rendered signatures to give the impression that electronic mail messages or other electronic communications were signed by the sender.

2.20.20 Forwarding Electronic Mail To An External Network Address

Unless the information owner/originator agrees in advance, or the information is clearly public in nature, workers must not forward electronic mail to any address outside MACRA's Network unless it is necessary in performing the employee's task.

2.20.21 Secret Information Sent By Email

Unless each occurrence is specifically authorized by the top management, readable secret information must not be sent by electronic mail. If encrypted with MACRA approved method, and if encrypted at the source and decrypted only at the destination, then secret information may be sent over an electronic mail system.

2.20.22 Disclaimer Of Responsibility Or Liability Notice For Message Content On Email Messages

Confidentiality and Disclaimer information should be indicated at the bottom of every outbound message in the email system.

MACRA specifically disclaims any responsibility or liability for the contents of any message sent by email. In these cases, MACRA is acting as a common carrier, and as such does not control the content of messages on the system. Likewise, MACRA does not verify the correctness, accuracy, or validity of the information appearing on this system.

2.20.23 Restriction On Forming Contracts Via Email

Correspondents with MACRA workers may in some cases construe an email message as a legally-binding statement. Unless specifically authorized to enter into contracts on behalf of MACRA, or otherwise authorized to legally represent MACRA, all workers must include a notice at the end of each email message indicating that the message does not bind MACRA to any contract, position, or course of action. The specific terms of this notice will be provided by the Legal Department and periodically be updated.

2.20.24 Restricted Behaviour for Outbound Email Communications

All outbound email communications must reflect well on MACRA's reputation and public image. Inflammatory, defamatory, harassing, disruptive communications, "spamming" and "flaming" is strictly prohibited.

2.20.25 Profane, Obscene or Derogatory Remarks In Electronic Mail Messages

Workers must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, or competitors. Such remarks—even when made in jest—may create legal problems such as trade libel or defamation of character. Special caution is warranted because backup and archival copies of electronic mail may actually be more permanent and more readily accessed than traditional paper communications.

Workers are prohibited from sending or forwarding any messages via MACRA information systems that a reasonable person would consider to be defamatory, harassing, or explicitly sexual. Workers are also prohibited from sending or forwarding messages or images via MACRA systems that would likely to offend on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability.

2.20.26 Reporting Offensive Electronic Mail Messages To Originator And HR

Workers are encouraged to respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications. If the originator does not promptly stop sending offensive messages, workers must report the communications to their manager and the Human Resources department.

2.20.27 Forwarding Is Appropriate Response To Junk Email (Spam)

When workers receive unwanted and unsolicited emails (also known as spam), they must not respond directly to the sender. Instead, they should forward the message to the email administrator or to the IT department who will take steps to prevent further transmissions.

2.20.28 Placement On Electronic Mail Distribution List

Nobody outside MACRA will be placed on any of MACRA's electronic mail distribution lists without first indicating their intention to be included on the list through an opt-in process.

2.20.29 Distribution Of Unsolicited MACRA Materials Through Email

Workers must not use electronic mail, other electronic systems (fax, dial-up devices), or any other communication systems for the distribution of unsolicited advertising material.

2.20.30 Prohibited Inbound Attachments To Internet Electronic Mail

Electronic mail messages sent to MACRA users which have attachments containing malicious software, or suspected malicious software, will be rejected or returned to the sender.

2.20.31 Prohibited Public and Free email accounts

Electronic mail messages sent to MACRA users which have originated from free and public email platforms shall be blocked for security and risk reasons.

2.21 Internet Usage Controls

2.21.1 Internet Privileges Reserved For Those With Business Need

Only those workers with supervisory levels and higher, who have received department management approval, may access the Internet via MACRA facilities. Approval will be granted after these workers have undergone the Internet policies and practices orientation seminar or as approved by the Head of IT and recommended by the worker's department head or immediate supervisor. Justification for internet access must be provided.

While electronic mail is provided to all workers, all other types of Internet access are reserved for those who have a demonstrable business need for such access. With the exception of electronic mail, all access to the Internet with MACRA information systems must be approved in advance in writing by the relevant department head.

Other workers may use the internet at their immediate supervisor's discretion or as required by their jobs.

Internet access for workers shall be terminated if the access is abused or misused in a way that hampers the operation of MACRA or puts the systems' integrity at risk.

2.21.2 Internet Use For Personal Purposes Prohibited On Authority Time

MACRA management allows workers to explore the Internet for growth, but if this exploration is for personal purposes, it must be done on personal, not Authority, time.

Downloading free software, viewing and obtaining pornographic materials, and similar activities are prohibited.

2.21.3 Internet Discussion Group And Chat Room Participation Forbidden

Unless expressly authorized by the Public Relations Department (or its equivalent), when using MACRA information systems, MACRA workers must not participate in Internet discussion groups, chat rooms, or public electronic forums.

2.21.4 Internet Representations Including MACRA Affiliation

When engaging in discussion groups, chat rooms, and other internet offerings, only those individuals authorized by management to provide official support for MACRA products and services may indicate their affiliation with MACRA. This may be accomplished explicitly by adding certain words to their messages, or implicitly via the use of an electronic mail address. In either case, unless they have received instructions to the contrary, whenever workers disclose affiliation with MACRA, they must clearly indicate that "the opinions expressed are my own and not necessarily those of my employer".

2.21.5 Disclaimer Must Accompany All Internet Personal Messages

When a worker posts a message to an Internet discussion group, an electronic bulletin board, or any other public information system, this message must be accompanied by words clearly indicating that the comments do not necessarily represent the position of MACRA. Such statements are required even when MACRA's name does not appear in the text of the message and/or when affiliation with MACRA has not been explicitly stated.

Exceptions will be made in those instances where the message has been approved for release by the Public Relations Department (or its equivalent).

2.21.6 Internet Representations About MACRA Products And Services

Workers must not advertise, promote, present, or otherwise make statements about MACRA products and services in Internet forums such as mailing lists, newsgroups, or chat sessions without the prior approval of the Public Relations Officer, Marketing Department (or it's equivalent).

2.21.7 Respecting Intellectual Property Rights Of Other Internet Users

Although the Internet is an informal communication environment, the laws for copyrights, patents, trademarks, and the like still apply. To this end, workers using MACRA systems must, for example:

- Post material only after obtaining permission from the source.
- Quote material from other sources only if these other sources are identified.
- Reveal internal MACRA information on the Internet only if the information has been officially approved for release.

2.21.8 Sending Software And Other Sensitive Information Over The Internet

Secret, proprietary, or private MACRA information must never be sent over the Internet unless it has first been encrypted by approved methods. Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.

2.21.9 Handling Of Software And Files Downloaded From Internet

All software and files downloaded from non-MACRA sources via the Internet (or any other public network) must be screened with virus detection software.

This screening must take place prior to the software or file being run or examine via another program such as a word processing package, and prior to its being moved to any other computer.

2.21.10 Exchanging Information Over The Internet

MACRA software, documentation, and all other types of internal information must not be sold or otherwise transferred to any other party for any purposes other than business purposes expressly authorized by management. Exchanges of software and/or data between MACRA and any third party may not proceed unless a written agreement has first been signed by MACRA DG.

2.21.11 Uploading Software To Other Machines Via The Internet

Users must not upload software that has been licensed by a third party, or software that has been developed by MACRA, to any computer via the Internet unless authorized by the Head of IT.

2.21.12 MACRA Blocks Certain Non-Business Internet Web Sites

MACRA information systems routinely prevent users from connecting with certain non-business websites. Workers using MACRA information systems who discover they have connected with a website that contains sexually explicit, racist, or other potentially offensive material must immediately disconnect from that website. The ability to connect a specific website does not in itself imply that workers are permitted to visit that site.

2.21.13 Reliability Of Information Down-Loaded From Internet

All information taken from the Internet should be considered suspect until confirmed by another source. There is no quality control process on the Internet and a considerable amount of Internet information is outdated, inaccurate, or deliberately misleading.

2.21.14 Production Systems Must Not Rely On Free Internet Information

Aside from information provided by prospects, customers, suppliers, business partners, or government agencies, MACRA information systems must not depend on free information obtained through the internet. This is because the timeliness, accuracy, author bias, and continued availability of such information are not reliable.

2.22 MACRA Internet Presence Controls

2.22.1 Internet Web Page Design Requirements

All MACRA Internet web pages must conform to layout standards, navigation standards, legal wording standards, and similar requirements specified by the management.

2.22.2 Disclaimer Of Responsibility Or Liability Notice For Message Content And Website

MACRA specifically disclaims any responsibility or liability for the contents of any message appearing on its website. In these cases, MACRA is acting as a common carrier, and as such does not control the content of messages on the system. Likewise, MACRA does not verify the correctness, accuracy, or validity of the information appearing on this system.

2.22.3 MACRA Internet Web Page Management Committee

Prior to being posted, all changes to MACRA corporate Internet web page must be approved by a special committee established by the Public Relations Department (or its equivalent). This committee will make sure that all posted material has a consistent and polished appearance, is aligned with business goals, and is protected by adequate security measures.

2.22.4 Accepting Unsolicited Ideas Through The Internet

If a mechanism to receive comments or suggestions is provided on the MACRA Internet website, it must be accompanied by the following words: “The receipt of unsolicited ideas by MACRA does not obligate MACRA to keep these ideas confidential, nor does it obligate MACRA to pay the person who submits them.”

2.22.5 Posting MACRA Material On The Internet

Users must not place MACRA material (software, internal memos, press releases, etc.) on any publicly-accessible Internet computer system unless the posting has been approved by the head of the Public Relations department (or its equivalent).

2.22.6 Digital Certificate For All MACRA Internet Web And E-Commerce Sites

A current digital certificate is required for every Internet server handling MACRA business to which customers, prospects, and others may connect.

2.22.7 Secret Information Must Not Be Placed On Internet Systems

Because Internet security technology keeps on changing, MACRA's secret information must not be stored on Internet servers.

2.22.8 Web And E-Commerce Servers Must Not Store Critical Information

Web and Commerce servers must not be used to store any critical MACRA business information.

2.22.9 All Internet Web Servers Must Be Firewall Protected

All web servers accessible via the Internet must be protected by a router or firewall approved by the IT Department.

All connections between MACRA internal networks and the Internet (or any other publicly-accessible computer network) must include an approved firewall and related access controls.

2.22.10 Internet Commerce Servers Must Use Digital Certificates And Encryption

To prevent intruders from interfering with Internet commerce activities, all Internet commerce servers (web servers, database servers, payment servers, security servers, etc.) must employ unique digital certificates and must use encryption to transfer information in and out of these servers.

An exception is made for web servers, FTP servers, and any other MACRA servers supporting communications with customers, prospects, or other members of the public.

2.22.11 Production Systems May Not Be Directly Internet Connected

In-house production information systems, such as core systems and other main servers, must not be directly connected to the Internet. Instead, these systems must connect with a commerce server, a database server, or some other intermediate computer that is dedicated to Internet business activity.

In cases where the production server is connected to the Internet to make use of the internet facility to establish links from and to branches through VPN (Virtual Private Network) or similar technology, full protection must be employed.

Firewalls or other forms of security must be installed in the system prior to allowing access to the production server through the internet.

2.23 Inbound Internet Access Controls

2.23.1 Extended User Authentication Required For In-Bound Internet Users

All users wishing to establish a connection with MACRA computers via the Internet must authenticate themselves at a firewall before gaining access to MACRA's internal network. This must be done via an extended user authentication process approved by the Head of IT. The use of extended user authentication systems will prevent intruders from guessing fixed passwords or from using a fixed password captured via a wiretap.

Designated "public" systems, such as Internet websites, do not need these authentication processes because anonymous interactions are expected.

2.23.2 Internet Access With MACRA Computers Must Go Through Firewall

Internet access using computers in MACRA offices is permissible only when users go through the MACRA firewall or equivalent protection. Other ways to access the Internet, such as dial-up connection with an internet service provider (ISP), are prohibited if MACRA computers are employed.

2.23.3 Permissible Internet Access Without Firewalls

Only one method is allowed for connections to the Internet without a firewall. This method involves the use of dial-up outbound connections from a stand-alone computer. When an in-house computer is connected to MACRA internal network, this machine must not simultaneously be connected to the Internet unless a firewall is employed.

2.23.4 Real-Time Connections To MACRA Production Systems Via Internet

The Internet must not be used to provide real-time connections to any of MACRA production systems that have extended user authentication access controls (i.e. controls beyond the fixed password and a user ID) unless the total protection has been established.

2.23.5 Approval Required For Access To Internal Systems By Third Parties

All third-party access to MACRA internal computer systems which are not clearly public (such as web servers containing MACRA brochures) must be approved in advance by the management.

2.23.6 Dial-Up Connections Must Always Utilize Firewalls

All inbound dial-up lines connected to MACRA's internal networks and/or computer systems must pass through an additional access control point (such as a firewall), which has been approved by the IT Department before users reach a log-in banner.

2.23.7 Real-Time External Network Connections Require Firewalls

All in-bound real-time external connections to MACRA Internet networks and/or multi-user computer systems must pass through an additional access control point (such as a firewall, gateway, or access server) before users reach a log-in banner.

2.23.8 Direct Network Connections with Outside Organizations (Tunnels)

The establishment of a direct connection between MACRA systems and computers at external organizations, via the Internet (through VPN) or any other public network, is prohibited unless this connection has been first approved by the Head of IT.

2.24 Network Controls

2.24.1 Internal Network Addresses And Configurations Must Not Be Publicly Released

The internal system addresses, configurations, and related systems design information or MACRA networked computer systems must be restricted so that both systems and users outside MACRA's internal network cannot access this information.

2.24.2 Access Control Packages Required For Computers On The Network

If workers leave the power for their computers turned on during non-business hours, and if such computers are connected to a network, the computers must be protected by an access control system approved by the Head of IT.

2.24.3 Access Control Packages For Network-Connected Computers

All MACRA computers that can be reached by third-party networks (including dial-up lines, value-added networks, the Internet, etc.) must be protected by a privilege access control system approved by the Head of IT.

This policy does not apply to computers that use modems to make outgoing dial-up calls, provided these systems do not receive unattended incoming dial-up calls.

2.24.4 Large Networks Must Be Divided Into Separate Domains

All large networks crossing national or organizational boundaries must have separately-defined logical domains, each protected with suitable security perimeters and access control mechanisms.

2.24.5 Internet-Connected Machines Must-Have Intrusion Detection Systems

To allow MACRA to promptly respond to attacks, all Internet-connected computers must be running an intrusion detection system approved by the IT Department.

2.24.6 All Firewalls Must Run On Dedicated Computers

All firewalls used to protect MACRA's internal network must run on separate dedicated computers. These computers may not serve other purposes, such as acting as web servers.

2.24.7 Firewall Configurations Change Requires Information Security Approval

Firewall configuration rules and permissible service rules have been reached after an extended evaluation of costs and benefits. These rules must not be changed unless the permission of the Head of IT has been obtained.

2.24.8 Trusted Host Relationship Prohibited For Internet Connected Machines

Unless the IT Department has approved, all MACRA computers that are internet-connected or directly reachable through the internet are prohibited from using shared directory systems (also called shared file systems). These systems allow a user to obtain access to more than one computer's file system with only a single log-in process.

Exceptions are made for internet commerce and other systems where multiple machine architecture involves automatically passing users with severely restricted privileges from one computer to another.

2.24.9 Isolate Systems Containing Secret Information From Network

MACRA computer systems containing secret information must not be connected to any network or any other computer.

2.24.10 Prior Approval Required For All Communication Line Changes

Workers and vendors must not make arrangements for, or actually complete the installation of voice or data lines with any carrier, if they have not first obtained approval from MACRA management.

2.24.11 Connecting To Third-Party Systems And Networks

MACRA's computers or networks may only be connected to third-party computers or networks after the IT Department has determined that the combined system will be in compliance with MACRA security requirements.

As a condition of gaining access to MACRA's computer network, every third party must secure its own connected systems in a manner consistent with MACRA requirements.

MACRA reserves the right to audit the security measures in effect on these connected systems without prior warning. MACRA also reserves the right to immediately terminate network connections with all third-party systems not meeting such requirements.

2.24.12 Approval Required To Establish Internet Connection

Unless prior approval of the Head of IT has been obtained, workers may not establish internet or any other external network connections which could allow another Authority's users to gain access to MACRA systems and information. These connections include the establishment of multi-computer file systems, Internet home pages, Internet FTP servers, and the like.

2.24.13 Inventory Of Connections To External Network

The IT Department must maintain a current inventory of all connections to external networks including telephone networks, intranets, extranets, and the Internet.

2.24.14 Modems On Workstations Connected To Internal Networks

Workers are prohibited from connecting dial-up modems to workstations that are simultaneously connected to a local area network (LAN) or another internal communications network. Approval by the Head of IT is required to determine security measures to be employed when such dial-up connection is necessary in performing business related to MACRA operations.

2.24.15 Secret Information Must Not Be Placed On Intranet Systems

Because intranet security technology keeps on changing, MACRA secret information must not be stored on intranet servers.

2.24.16 Webmaster Review Of Intranet Web Pages Prior To Posting

Prior to being posted to the MACRA intranet, all user-developed web pages must be tested for security and operational problems according to an approved process by the management.

2.24.17 Forwarding Information On MACRA Intranet To Third Parties

MACRA intranet is for the exclusive use of authorized persons. Unlike the Internet, information on the intranet may be disseminated only to authorized persons. Workers must not forward information appearing on the intranet to third parties without going through the appropriate internal channels (such as Human Resources, Marketing, Public Relations, and IT).

2.25 General Security Controls

2.25.1 Mobile Devices Used For Corporate Business Information

Personal computers, smartphones, digital cameras, and other handheld devices must not be used for MACRA business information unless they have first been configured with necessary controls and approved for such use by the IT Department. Exceptions will be made for calendars, address books, to-do tasks, and stored connection information such as telephone numbers.

2.25.2 Power Down Required For Systems Processing Sensitive Information

All computers that have been used for processing secret information must be powered down at the end of the day, at lunch break, at the termination of a session, or when not in use. In most cases, this will erase residual information contained in the computer's memory (check the manufacturer's documentation to make sure), preventing it from being disclosed to unauthorized parties. An exception may be made for stand-alone computers located in areas with strict physical access controls which prevent unauthorized persons from gaining access to the system.

2.25.3 Controls For Transportable Computers

Workers using portable computers (such as laptops and iPads) containing MACRA information must not leave these computers unattended at any time unless the secret information has been encrypted.

All portables, laptops, notebooks, and other transportable computers containing MACRA's sensitive information must consistently employ both hard disk encryptions for all files as well as boot protection.

Workers in the possession of transportable computers containing sensitive MACRA information must not check these computers in airline luggage systems. These computers must remain in the possession of the traveller as hand luggage unless restricted by airport security regulations.

2.26 Audit Controls

2.26.1 Internal Audit Review Of Information System Controls

The Internal Audit Division must periodically review the adequacy of information system controls as well as compliance with such controls.

2.26.2 Internal Audit Performs Information Security Compliance Checking

The Internal Audit Division must periodically perform compliance checking related to information security policies, standards, and procedures.

2.26.3 Periodic MACRA Review Of Information Systems Controls

MACRA IT Departmetn and MACRA Audit Division must periodically perform compliance checking related to information security policies, standards, and procedures.

2.26.4 Periodic Independent Review Of Information System Controls

An independent and externally-provided review of information system controls must be periodically obtained. These reviews must include efforts to determine both the adequacy of and compliance with, controls. The reviews must not be performed by persons responsible for implementing and maintaining controls.

2.26.5 Audit Trails Required

All systems implemented in MACRA must conform to the audit requirements. Audit trails must be employed by MACRA to be available in the system before the system will be developed or acquired.

2.26.6 Systems Audit Required

All systems developed or acquired must pass the systems auditing standards and practices or as initially required by the Internal Systems Auditor.

2.27 Reporting of Security Problems

2.27.1 Centralize Reporting Of Information Security Problems

All known vulnerabilities—in addition to all suspected or known violations—must be communicated in an expeditious and confidential manner to the IT department.

Unauthorized disclosures of MACRA information must additionally be reported to the involved information owners.

Reporting security violations, problems or vulnerabilities to any party outside MACRA without the prior written approval by the management is strictly prohibited.

2.27.2 Systems Designers & Developers Must Inform Management Of Problems

All potentially serious problems associated with information systems being designed or developed, that are not being adequately addressed by planned or existing projects, must be promptly reported to the management.

2.27.3 Annual Analysis Of Information Security Violations & Problems

An annual analysis of reported information security problems and violations must be prepared by the IT department and reviewed by the Internal Audit Division.

3 PC and Network Usage Declaration

- I agree to change my password every 90 days. I also agree that my password will comprise at least 8 characters (I will use small and capital characters as well as numbers and special characters) in
  accordance with Information Technology Policies and Procedures at MACRA.

- I will not write my password down or tell it to anyone.

- The main computer room and the communication closets found throughout the building are off limits

  to all non-IT employees. I will not attempt entry into these areas.

- I will not insert floppy disks or USB drives into any desktop or use the CD-ROM player without prior approval from the Head of IT. Any floppy disk or USB drive used outside MACRA's premises must

be scanned for viruses prior to their contents being copied on a specific folder on a server.

- I will not attempt to disable the network nor the system in any way.

- I will not attempt to install any software onto any PC belonging to the Authority.

- I will not attach any unauthorized device to the network.

- I will not use the Authority's computer equipment for anything other than official Authority business.

- Violating any of these rules will result in restriction of network usage or disciplinary action by the

  management of MACRA.

Employee Name: ____________________

Department: ____________________

Date: ____________________

Signature: ____________________