**REPUBLIC OF RWANDA**

****

**MINISTRY OF GENDER**

**AND FAMILY PROMOTION**

MIGEPROF ICT POLICY AND PROCEDURE

**December 2016**

Contents

[**INTRODUCTION** 5](#_Toc488652156)

[**Section 1: EMAIL AND INSTANT MESSAGING** 6](#_Toc488652157)

[1.1 General instructions: 6](#_Toc488652158)

[1.2. Ownership instructions 7](#_Toc488652159)

[1.3. Confidentiality instructions 7](#_Toc488652160)

[1.4. Security instructions 8](#_Toc488652161)

[1.5. Inappropriate use 8](#_Toc488652162)

[**Section 2: INTERNET USAGE** 10](#_Toc488652163)

[2.1. General instructions 10](#_Toc488652164)

[2.2. Inappropriate use 10](#_Toc488652165)

[**Section3: PASSWORD SECURITY** 12](#_Toc488652166)

[3.1. Password Guidelines 13](#_Toc488652167)

[**Section 4: SOFTWARE USAGE** 14](#_Toc488652168)

[4.1. General 14](#_Toc488652169)

[4.2. Compliance 14](#_Toc488652170)

[4.3. Registration of software 15](#_Toc488652171)

[4.4. Software Audit 16](#_Toc488652172)

[**Section5: PC SOFTWARE STANDARDS** 17](#_Toc488652173)

[5.1. Applicability 17](#_Toc488652174)

[5.2. Technical Support 17](#_Toc488652175)

[5.3. ICT network Officer’s Role in the Purchase of Hardware and Software 17](#_Toc488652176)

[4. Requesting Standard PC Equipment and Software 18](#_Toc488652177)

[5. Request for a Variance from the PC Hardware or Software Standard 18](#_Toc488652178)

[**Section 6: INVENTORY AND EQUIPMENT** 19](#_Toc488652179)

[6.1. Allocating equipment to employees 19](#_Toc488652180)

[6.2. Employee termination 19](#_Toc488652181)

[6.3. Technology assets 19](#_Toc488652182)

[**Section 7: PC STANDARDS** 20](#_Toc488652183)

[7.1. General instructions 20](#_Toc488652184)

[7.2. Network access 20](#_Toc488652185)

[7.3. PC Support 20](#_Toc488652186)

[7.4. Employee training 20](#_Toc488652187)

[7.5. Backup procedures 21](#_Toc488652188)

[7.6. Virus software 21](#_Toc488652189)

[7.7. Applications software 21](#_Toc488652190)

[**Section 8: IMAGING DEVICE USAGE** 22](#_Toc488652191)

[8.1. Printer Usage 22](#_Toc488652192)

[8.2. Photocopy Usage 22](#_Toc488652193)

[**Section 9: INFORMATION SECURTY** 23](#_Toc488652194)

[9.1. Data classification 24](#_Toc488652195)

[9.2. Access control 25](#_Toc488652196)

[9.3. Virus prevention 26](#_Toc488652197)

[9.4. Intrusion detection 26](#_Toc488652198)

# **INTRODUCTION**

MIGEPROF ICT Policy and Procedure Manual provide the policies and procedures to be followed by MIGEPROF’s staff for effectively use of ICT facilities within Ministry. It also provides guidelines the Ministry will use to administer these policies, with the correct procedure to follow.

MIGEPROF in line with National laws and regulations will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures and policy.

These policies and procedures apply to all employees of MIGEPROF.

# **Section 1: EMAIL AND INSTANT MESSAGING**

This section provides appropriate guidelines for productively utilizing the MIGEPROF's email system and instant messaging technology that protects the employee and institution while benefiting from MIGEPROF systems.

MIGEPROF has established this policy with regard to the acceptable use of provided electronic messaging systems, including but not limited to email and instant messaging.

The Email and instant messaging are important and sensitive tools. This policy applies to any and all electronic messages composed, sent or received by any employee or by any person using MIGEPROF provided electronic messaging resources. MIGEPROF sets forth the following policies/instructions but reserves the right to modify them at any time in order to support Ministry.

## 1.1 General instructions:

* MIGEPROF provides electronic messaging resources to assist in conducting

 Good work and communication.

* All messages composed and/or sent using MIGEPROF provided electronic messaging resources must comply with this policies regarding acceptable communication.
* Use of electronic messaging resources to discriminate for any or all of these following forms of discrimination is prohibited. Discrimination based on age, race, gender, sexual orientation, religious or political beliefs.
* Upon termination or separation from Ministry, MIGEPROF will deny all access to electronic messaging resources, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.
* Each employee will be assigned a unique email address that is to be used while conducting MIGEPROF work via email.
* Employees authorized to use instant messaging programs will be advised specifically on which instant message program(s) are permissible.
* Employees authorized to use instant messaging programs will be assigned a unique Instant messaging identifier, also known as a buddy name, handle or nickname.
* Electronic messages are frequently inadequate in conveying mood and context. Carefully consider how the recipient might interpret a message before composing or sending it.
* Any employee who discovers a violation of these policies should immediately notify Human Resources specialist.
* Any employee in violation of these policies is subject to disciplinary action, including but not necessarily limited to termination.

## 1.2. Ownership instructions

* The e-mail/electronic messaging systems are MIGEPROF property. All messages stored in MIGEPROF provided electronic messaging system(s) or composed, sent or received by any employee or non-employee are the property of the MIGEPROF. The Electronic messages are NOT the property of any employee.
* The MIGEPROF reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received.
* The MIGEPROF reserves the right to alter, modify, re-route or block the delivery of messages as appropriate.
* The unique email addresses and/or instant messaging identifiers assigned to an employee are the property of the MIGEPROF. Employees may use these identifiers only while employed by MIGEPROF.

## 1.3. Confidentiality instructions

* Messages sent electronically can be intercepted inside or outside the MIGEPROF and as such there should never be an expectation of confidentiality. Do not disclose proprietary or confidential information through email or instant messages.
* Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in Determining whether a message should be delivered electronically versus in person.
* Electronic messages are legally discoverable and permissible as evidence in a court of law. Messages should not be composed that you would not want to read out loud in a court of law.
* Employees are prohibited from unauthorized transmission of MIGEPROF trade secrets, confidential information or privileged communications.
* Unauthorized copying and distribution of copyrighted materials is prohibited.

## 1.4. Security instructions

* MIGEPROF employs sophisticated anti-virus software. Employees are prohibited from disabling anti-virus software running on MIGEPROF provided computer Equipment.
* Although the MIGEPROF employs anti-virus software, some virus infected messages can enter the MIGEPROF’s messaging systems. Viruses, “worms” and other malicious code can spread quickly if appropriate precautions are not taken. Follow the precautions discussed below:
* Be suspicious of messages sent by people not known by you.
* **Do not open attachments** unless they were anticipated by you. If you are not sure, always verifythe sender is someone you know and that he or she actually sent you the email attachment.
* Disable features in electronic messaging programs that automatically preview Messages before opening them.
* Do not forward chain letters. Simply delete them.
* The MIGEPROF considers unsolicited commercial email (spam) a nuisance and a potential security threat. Do not attempt to remove yourself from future delivery of a message that you determine is spam. These “Remove Me” links are often used as a means to verify that you exist.
* Internet message boards are a fertile source from which mass junk E-mailers harvest E-mail addresses and email domains. Do not use MIGEPROF provided email addresses when posting to message boards.

## 1.5. Inappropriate use

* Email or electronic messaging systems may not be used for transmitting messages containing pornography, profanity, derogatory, defamatory, sexual, racist, harassing, or offensive material.
* MIGEPROF provided electronic messaging resources may not be used for the promotion or publication of one’s political or religious views, the operation of a business or for any undertaking for personal gain.

# **Section 2: INTERNET USAGE**

This section provides appropriate guidelines for accessing and utilizing the Internet through network.

Internet services are authorized to designated employees to enhance their job responsibility. The Internet is an excellent tool but also creates security implications that MIGEPROF must guard against. For that reason, employees are granted access only as a means of providing support in fulfilling their job responsibility.

## 2.1. General instructions

* Internet accounts are approved for MIGEPROF’s employee to provide tools that assist in their work.
* Each individual is responsible for the account issued to him/her.
* Sharing Internet accounts or User-ID's is prohibited.
* Organizational use of Internet services must reflect the mission of MIGEPROF and support the MIGEPROF's goals and objectives.
* These services must support legitimate, mission related activities of the MIGEPROF and be consistent with prudent operational, security, and privacy considerations.
* Information, Education, Communication specialist and ICT network officer will take responsibility for all website content (" MIGEPROF website") and format presentation to reflect the MIGEPROF's mission and in supporting MIGEPROF and units objectives.
* MIGEPROF has no control over the information or content accessed from the Internet and cannot be held responsible for the content.
* Any software or files downloaded via the Internet into the network become the property of the MIGEPROF. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

## 2.2. Inappropriate use

The following uses of MIGEPROF provided Internet accesses are not permitted:

* To access, upload, download, or distribute pornographic or sexually explicit material
* Violate and state, local, or federal law
* Vandalize or damage the property of any other individual or organization
* To invade or abuse the privacy of others
* Violate copyright or use intellectual material without permission
* To use the network for financial or commercial gain
* To degrade or disrupt network performance
* No employee may use MIGEPROF facilities knowingly to download or distribute pirated software or data. The use of file swapping software on MIGEPROF computers and networks is prohibited.
* No employee may use the MIGEPROF’s Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

# **Section3: PASSWORD SECURITY**

This section provides guidelines in appropriate management of Ministry passwords to maintain adequate security and integrity of all of ministry's systems. Maintaining security of applications, software tools, email systems, network facilities, and voice mail are critical to provide data integrity and stability of MIGEPROF systems.

* The Ministry provides access to network, electronic mail and voice mail resources to its employees in support of the MIGEPROF's mission. Passwords are assigned for access to each of these resources to authenticate a user's identity, to protect network users, and to provide security.
* It is the responsibility of each individual to protect and to keep private any and all passwords issued to him/her by MIGEPROF.
* ICT network Officer will establish guidelines for issuing new passwords, deleting Passwords as required, and allowing employees to change their passwords.
* Although the MIGEPROF strives to manage a secure computing and networking environment, the MIGEPROF cannot guarantee the confidentiality or security of network, e-mail or voice mail passwords from unauthorized disclosure.
* New employee passwords and changes must be requested by his director. This

Helps monitor and manage the importance of protecting passwords in their distribution and use in such a way that reinforces the integrity of users accessing MIGEPROF systems.

* ICT network Officer must approve any password change requested by a user's Director. Confirmation will be sent to user when a password change is completed at the request of Director.
* ICT network Officer will handle all support requests from MIGEPROF employees.
* ICT network Officer will delete all passwords of exiting employees upon notification from Human Resources.
* ICT network Officer and users assume the following responsibilities:
* ICT network Officer must protect confidentiality of user’s password.
* User must manage passwords according to the Password Guidelines.
* User is responsible for all actions and functions performed by his/her account.
* Suspected password compromise must be reported to ICT network Officer immediately.

## 3.1. Password Guidelines

* **Select a Wise Password**

 To minimize password guessing:

* Do not use any part of the account identifier (username, login ID, etc.).
* Use 8 or more characters.
* Use mixed alpha and numeric characters.
* Use two or three short words that are unrelated.
* **Keep Your Password Safe**
* Do not tell your password to anyone.
* Do not let anyone observe you entering your password.
* Do not display your password in your work area or any other highly visible place.
* Change your password periodically (every 3 months is recommended).
* Do not reuse old passwords.
* **Additional Security Practice**

Ensure your workstation is reasonably secure in your absence from your office.

Consider using a password-protected screen saver, logging off or turning off your Monitor or laptop when you leave the office

# **Section 4: SOFTWARE USAGE**

This section provides guidelines on appropriate use of software products utilizing by MIGEPROF equipments. This policy is intended to ensure that all MIGEPROF employees understand that no computer software may be loaded onto or used on any computer owned or leased by MIGEPROF unless the software is the property of or has been licensed by the known and accepted vendor.

## 4.1. General

* Software purchased by the MIGEPROF or residing on MIGEPROF owned computers is to be used only within the terms of the license agreement for that software title. Unless otherwise specifically provided for in the license agreement, any duplication of copyrighted software, except for archival purposes is a violation of copyright law.
* To purchase software, users must obtain the approval of their Directors who will follow the same procedures used for acquiring other MIGEPROF assets.
* All approved software will be purchased through procurement.
* ICT network Officer will be the sole governing body for defining appropriate software titles acceptable for use in the MIGEPROF.
* Under no circumstances will third party software applications be loaded onto MIGEPROF owned computer systems without the knowledge of and approval of the ICT Network Officer.
* Illegal reproduction of software is subject to civil and criminal penalties, including fines and imprisonment. Any MIGEPROF user, who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances and may include termination of employment.
* MIGEPROF does not condone the illegal duplication of software in any form.

## 4.2. Compliance

* MIGEPROF will use all software in accordance with its license agreements.
* Legitimate software will be provided to all users who need it. MIGEPROF users will not make unauthorized copies of software under any circumstances. Anyone found Copying software other than for backup purposes is subject to termination.
* Each user of software purchased and licensed by the MIGEPROF must acquire and use that software only in accordance with the applicable Software License Agreement.
* All users acknowledge that software and its documentation are not owned by the MIGEPROF or an individual, but licensed from the software publisher.
* Employees of MIGEPROF are prohibited from giving MIGEPROF acquired software to anyone who does not have a valid software license for that software title. This shall include but is not limited to clients, vendors, colleagues, and fellow employees.
* All software used by a MIGEPROF entity for MIGEPROF owned computing devices, or purchased with MIGEPROF funds, will be acquired through the appropriate procedures.
* Any user who determines that there may be a misuse of software within the organization will notify ICT network Officer.

## 4.3. Registration of software

* Software licensed by the MIGEPROF will not be registered in the name of an individual.
* When software is delivered, it must first be properly registered with the software publisher via procedures appropriate to that publisher. Software must be registered in the name of the MIGEPROF with the job title or Unit name in which it is used. After the registration requirements above have been met, the software may be installed in accordance with the policies and procedures of the MIGEPROF. A copy of the license agreement will be filed and maintained by the ICT network Officer.
* Once installed, the original installation media should be kept in a safe storage area designated by ICT network Officer.
* Shareware software is copyrighted software that is distributed freely through bulletin boards, online services, and the Internet. MIGEPROF's policy is to pay shareware authors the fee they specify for use of their products if the software will be used at the MIGEPROF. Installation and registration of shareware products will be handled the same way as for commercial software products.

## 4.4. Software Audit

* ICT network Officer will conduct periodic audits of all MIGEPROF owned PCs, including laptops, to insure MIGEPROF is in compliance with all software licenses.
* Audits will be conducted using an auditing software product. Software for which there is no supporting registration, license, and/or original installation media will be removed immediately from the user's computer. During these audits, ICT network Officer will search for computer viruses and eliminate any that are found.
* The full cooperation of all users is required during software audits.

# **Section5: PC SOFTWARE STANDARDS**

This section provides guidelines for purchasing and installing software on MIGEPROF PC's. The purpose for this policy is to explain MIGEPROF PC and software standards and to identify the levels of technical support available to MIGEPROF employees from ICT network Officer

## 5.1. Applicability

This policy applies to all employees of the MIGEPROF requesting the purchase of

New computer software and who desire computing support for that application from ICT network Officer. The following software standards have been established to ensure efficient and

 Cost effective use of MIGEPROF computing assets:

* To help ensure compatibility between applications and releases
* To provide more effective system administration
* To assist in the computer planning process and enable the realization of

Long term goals and the future computing vision

* To ensure cost effective purchasing
* To enable effective tracking of software licenses
* To provide cost effective end user software training
* To facilitate efficient and effective technical support effort

## 5.2. Technical Support

* Software support is provided at several levels and is based on whether the software is the MIGEPROF enterprise standard or unit specific.
* ICT network Officer will not provide support for evaluation software, personally Purchased software, illegal copies of software, screen savers, shareware, and non-network software that is not included in the standard software list.
* Software applications determined by ICT network Officer to cause computer problems with standard network software will be removed.

## 5.3. ICT network Officer’s Role in the Purchase of Hardware and Software

* Assist Unit with evaluating new business software solution.
* Act as liaison for Units when dealing with computing vendors.
* Recommend and evaluate the tasks/jobs/functions to be accomplished via the new software product.
* Assist with hardware and system requirements.
* Install the software as needed.

## 4. Requesting Standard PC Equipment and Software

* Equipment and software requests that are covered by the MIGEPROF's PC Equipment and Software Standards List will be provided quickly as long as appropriate approvals are granted.
* The steps that follow outlines the process for purchasing PC equipment and software:
1. Write Memo Request.
2. Gain approval of unit Director.
3. Submit request to ICT network Officer.
4. ICT network Officer will review the Memo and forward it to Procurement for purchasing or will contact Requestor for clarification as needed.
5. ICT network Officer is available for follow-up questions regarding your order as needed.

## 5. Request for a Variance from the PC Hardware or Software Standard

1. Write a Memo “Request for a Variance from the PC Hardware and Software Standard".
2. Practical and sufficient justification is a key part so be concise in building your case for deviating from the standard.
3. Gain approval of the request from Human resource.
4. Submit the request to the ICT network Officer for review.
5. Your request is reviewed and either approved or declined based upon justified reasons presented and ICT network Officer’s ability to support the new configuration within the network.

# **Section 6: INVENTORY AND EQUIPMENT**

This section provides management guidelines for managing the use and security of MIGEPROF’s inventory and equipment. PC's, equipment, and supplies are purchased for MIGEPROF employee use and productivity. It is the responsibility of all employees and Director of unit to manage the security of MIGEPROF equipment and supplies in order to manage effectively the Ministry's assets.

## 6.1. Allocating equipment to employees

* Equipment is assigned to employees based upon their job function.
* ICT network Officer should maintain a list of equipment allocated to each office.
* Specific equipment should be tracked by employee includes, but is not limited to:
* PC's (both desktop and laptop)
* PC peripherals (scanners, printers, modems, etc.)

## 6.2. Employee termination

* One of the responsibilities of the Director of unit is to collect all allocated equipment issued to an employee who leaves MIGEPROF.
* Employees not able to return allocated equipment are responsible for reimbursing the MIGEPROF on the fair market value of the item.

## 6.3. Technology assets

ICT network Officer will maintain an accurate inventory of all networked technologyassets, laptops, and tangible technology equipment of MIGEPROF to include the following information:

* Item model
* Serial Number
* Physical location
* Technology equipment will be tagged for easy identification.
* Quarterly periodic inventory audits will be conducted to validate the inventory and to identify maintenance issues needed for employee productivity.

# **Section 7: PC STANDARDS**

This section provides guidelines for maintaining a standard PC image for the Ministry that addresses the needs of MIGEPROF employees**.** MIGEPROF will maintain standard configurations of PC's and laptops in order to enhance employee productivity and supportability of network.

## 7.1. General instructions

* ICT network Officer will establish the standard configuration of PC hardware and software to be run on MIGEPROF PC's and laptops.
* Multiple configurations are maintained to provide stronger capabilities for employees that need more PC capabilities for their work. These users are called "Power users" and are determined to need the more capable PC's by human resource.

## 7.2. Network access

* All PC's are network enabled to access the network.
* It is the employee's responsibility to maintain appropriate security measures when accessing the network as defined in the MIGEPROF's Password Securitypolicy.

## 7.3. PC Support

* ICT network Officer will maintain all PC's of the MIGEPROF or will direct to appropriate measures for maintaining the PC.
* Standard configurations are defined to assist in providing responsive support and to assist in troubleshooting the issue or problem. Deviations from the standards are not permitted except in appropriately reviewed and approved situations.
* For assistance with the PC or peripheral equipment, contact ICT network Officer.

## 7.4. Employee training

Basic training for new employees on the use of PC's, accessing the network, and using applications software is held by ICT network Officer.

## 7.5. Backup procedures

Data and software on the PC is not backed up. If a staff wants to protect data and files used on his/her PC, he/she should take one of the following measures:

Save the data on CDs or external Hard disk.

## 7.6. Virus software

* MIGEPROF maintains network antivirus software that will automatically scan your PC for possible viruses each time you log onto the network.
* Downloading or copying data files from external systems and the Internet are prohibited without scan of that external system to protect the integrity of network.

## 7.7. Applications software

* Standard software is maintained on all PC's and laptops.
* Under no circumstances are additional software programs allowed to be loaded onto a PC without the review and approval of ICT network Officer. This is a protective measure to avoid network problems due to viruses and incompatibility issues.

# **Section 8: IMAGING DEVICE USAGE**

## 8.1. Printer Usage

In order to reduce the use and the cost of paper in accordance with Government of Rwanda’s vision in ICT and increase productivity within the Ministry of gender and Family Promotion ; all staff will proceed with:

* Print documents related to work purposes only,
* Print on both sides wherever it is possible
* Use a networked printer made available by the Ministry of gender and Family Promotion within close proximity to their work area and additional printers may be given where necessary.
* Ensure that the document to print is at its final draft and set number of copies required
* Ensure that confidential and critical information which is printed is collected from the printer immediately;
* Avoid the intrusion of staples, paper clips, or other foreign objects to pass through the printing machines
* Shutdown printers at the end of each working day

## 8.2. Photocopy Usage

* Copy documents related to work purposes only
* Avoid the intrusion of staples, paper clips, or other foreign objects to pass through the photocopying machine.
* Ensure that the photocopy is set for the required setting mode and paper copy quantity before beginning photocopying and copying on both sides whenever possible is recommended.
* Collect confidential information after being photocopied from the photocopy immediately.
* Shutdown photocopying machine at the end of each working day
* Report any malfunction to ICT Network Officer
* Always read and analyse any message displayed on printer’s screen or on computer’s screen.

# **Section 9: INFORMATION SECURTY**

This section provides guidelines those protect the data integrity and proprietary nature of the information systems of MIGEPROF. By information security we mean protection of the MIGEPROF's data, applications, networks and computer systems from unauthorized access, alteration or destruction.

* The purpose of the information security policy is:
* To establish a MIGEPROF-wide approach to information security.
* To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of MIGEPROF data, applications, networks and computer systems.
* To define mechanisms that protects the reputation of the MIGEPROF and allows MIGEPROF to satisfy its legal and ethical responsibilities with regard to its computer systems' connectivity to worldwide networks and networks'.
* To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.
* MIGEPROF will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the MIGEPROF’s data, network and system resources.
* The information security policy is updated on a regular basis and published as appropriate.
* Appropriate training is provided to data owners, data custodians and users.
* Each Unit must appoint a person responsible for security, incident response, periodic user access reviews, and education of information security policies for the department.
* Vulnerability and risk assessment tests of external network connections should be conducted on a regular basis.
* Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data.
* Violation of the Information Security Policy may result in disciplinary actions as Authorized by the MIGEPROF.

## 9.1. Data classification

* It is essential that all MIGEPROF data be protected. Different types of data require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance.
* The MIGEPROF classifies data in the following three classes:
* **High Risk:** Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Like Payroll, personnel, and financial information are also in this class because of privacy requirements.
* MIGEPROF recognizes that other data may need to be treated as high risk because it would cause severe damage to the MIGEPROF if disclosed or modified.
* The data owner should make this determination. It is the data owner’s responsibility to implement the necessary security requirements.
* **Confidential** – Data that would not expose MIGEPROF to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner’s responsibility to implement the necessary security requirements with the help of ICT Network Officer.
* **Public** - Information that may be freely disseminated. All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the MIGEPROF.
* Data owners must determine the data classification and must ensure that ICT network Officer is protecting the data in a manner appropriate to its classification level.
* No MIGEPROF owned system or network can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
* High risk and confidential data must be encrypted during transmission over insecure channels.
* All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
* Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or re-purposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

## 9.2. Access control

* Data must have sufficient granularity to allow the appropriate authorized access.
* There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized and addressed appropriately.
* MIGEPROF will have a standard policy that applies to user access rights. This will suffice for most instances.
* Data owners may enact more restrictive policies for end-user access to their data.
* Access to the network and systems will be achieved by individual and unique logins, and will require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.
* As stated in the Appropriate Use Policy, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system from unauthorized use.
* All users of systems that contain high risk or confidential data must have a strong Password. Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by ICT network Officer.
* Passwords must not be placed in emails unless they have been encrypted.
* Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
* Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
* Users are responsible for safe handling and storage of all MIGEPROF authentication devices. Authentication tokens (such as wireless password) should not be stored with a computer that will be used to access the MIGEPROF’s network or system resources.
* If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.
* Terminated employee access must be reviewed and adjusted as found necessary.
* Terminated employees should have their accounts disabled upon transfer or termination.
* Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the ICT network Officer.
* Transferred employee access must be reviewed and adjusted as found necessary.
* Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.
* Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks.
* There should be a documented procedure for reviewing system logs.

## 9.3. Virus prevention

* The willful introduction of computer viruses or disruptive/destructive programs into MIGEPROF environment is prohibited, and violators may be subject to prosecution.
* All IT systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor’s recommendations.
* Where feasible, ICT network officer should inform users when a virus has been detected.
* Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

## 9.4. Intrusion detection

* Intruder detection must be implemented on workstations containing data classified as high or confidential risk.
* Operating system and application software logging processes must be enabled on all host systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
* Intrusion Detection tools should be installed where appropriate and checked on a regular basis.

**Enforcement**

Any employee found to have violated this policy may be subject to disciplinary sanction up to and including termination of employment.