ICT Security Policy and Procedures

Office Address: Sunnyside Office Park
Sentinel House, 2nd floor.
32 Princess of Wales,
Parktown,
Johannesburg2196
Telephone: +27 11 026 7323 Email:
website@responsiblegambling.org.za
Website: www.respomsiblegambling.org.za

Document History and Approvals

Version	**2024**
Reference Number	**SARGF/2024**
Date Completed	**Sept 2024**
Revision Number	**1**
Date Issue	**Sept 2024**
Compiled By	**Mrs. Sibongile Simelane-Quntana** **Executive Director** **Signature: _____** **Date:**
Recommendations	**Audit and Risk Committee** **Chairperson: Mr. Thabani Khanyile** **Signature: _____** **Date:**
Approval	**SARGF Board** **Chairperson: Advocate Fana Nalane** **Signature: _____** **Date:**

Table of Contents

1. Objective

This policy is aimed at managing the potential risk of the South African Responsible Gambling Foundation's data, computer systems, platforms and Network services. Additionally, the purpose of this policy is to ensure that Users are aware of their responsibilities (and the potential consequences of a breach of these responsibilities) to the South African Responsible Gambling Foundation (SARGF).

2. Scope

This document records SARGF's policy with regard to compliance with relevant data protection legislation and other relevant legislation and it governs the following areas:

2.1 correct and proper usage by Users of SARGF's data, computer system and Network services;
2.2 Users' access to the internet provided by the SARGF; and
2.3 E-mail sent and received by Users through the organisations e-mail system.

The terms and conditions described in this policy apply to all Users of SARGF's data, computer systems and Network services. This policy should be read in conjunction with the other policies specifically referred to in this document, which can be obtained from the Finance and Administration Unit.

3. Policy Preamble and General Terms

3.1 The objectives of the policy are:

3.1.1. To increase awareness of electronic data or information security among management and staff;
3.1.2. To encourage ethical and lawful behavior by Users and providers of information
3.1.3. To detail the consequences of inappropriate use of SARGF's data and/or resources;
3.1.4. To provide a guideline for protecting information resources from theft, loss, damage and unauthorised access or change; and
3.1.5. To increase awareness of the confidentiality of SARGF's data, confidential material and information

3.2 General Terms

3.1.6. The terms and conditions described in this policy apply to all Users of the organisations.
3.1.7. Each component of the SARGF computer system, be it owned, leased, rented, or borrowed by SARGF, will remain the exclusive property and under control of the organisation, and will be provided to the User at the organisation's expenses.
3.1.8. The SARGF computer systems and all data thereon are critical business assets and mistreatment or abuse thereof by a User may, in SARGF's discretion, render such User liable for disciplinary action in accordance with SARGF's disciplinary procedures, as amended from time to time.
3.1.9. In conducting their work as required by the SARGF and in their interaction and dealings with internal and external stakeholders, Users should be

aware that in so doing they are representing the interest of SARGF as such the use of computer system which may carry identification of the SARGF may be possibly bind SARGF may carry some obligations and/or liability on behalf of the organisation and/or the User.

3.1.10. It is every User's responsibility to use the organisation's computer system and data responsibly, professionally, ethically, and lawfully, and to use every endeavor to promote and ensure the confidentiality, integrity and availability of data and information internally and externally.

3.1.11. Use of the SARGF computer system is provided primarily to assist Users in the performance of their work function for, and on behalf of, SARGF. Certain limited personal users, as contemplated in terms of this policy, is at the absolute discretion of the organisation and no User may claim such personal use as a right.

3.1.12. In terms of this policy specified personnel may access and review all materials that the User has created, stored, sent or received on the organisation computer system, whether through the Internet, e-mail and or otherwise. In addition, the organisation may from time to time use human or automated means to monitor the use of its computer resources.

3.1.13. The User accepts that the access, review and monitoring referred to above will be performed by the organisation (in its sole discretion) at such times as it deems fit.

3.1.14. Supporting standards, guidelines and procedure will be issued on an ongoing basis by SARGF. Users have an obligation to obtain the current policies from the SARGF Intranet (Shared Drive) on an ongoing basis and accept the terms and conditions therein.

4 Policy Requirements

4.1 Access

Users shall only access SARGF's computer system on the following terms and conditions:

4.1.1. Access to computer equipment will only be granted by the Finance and Administration Unit upon receipt of a signed user access form by both the manager and the user.

4.1.2. Access to the organisation data system shall only be accessed by means of equipment that meets the ICASA safety standards. In an event that Users to use, their own or other equipment they must ensure that such equipment is safe for use and that it meets the ICASA safety standards. , Remote access to the organisation computer system from outside the organisation premises shall only be attempted by way of remote or laptop facilities provided by SARGF utilizing a software provided by the organisation; and

4.1.3. Remote access shall be granted to Users at the sole discretion of the organisation and on the terms and conditions that the Executive Director, in his/her discretion, shall determine.

4.2 Authorised users only use assigned usernames and passwords.

4.2.1. Users may only access the SARGF computer system, e-mail and Internet facilities by means of their authorized usernames and passwords.

4.2.2. Apart from staff members authorised by the Executive Director, Users shall not use any other username or password other than their username and password.

4.2.3. Users shall not knowingly allow the use of their username and/or passwords by anyone else, whether such other person is an authorised User or not.

4.2.4. Users are alerted to the fact that they are responsible for all work saved or retrieved, messages sent or received, or transactions carried out under their username and password; and

4.2.5. Users shall report any instance or suspicions of a third party requesting their password, regardless of the requestor, to the Finance and Administration Manager

4.3 Passwords

To prevent unauthorised access to the organisation's computer system, passwords shall comply with the following standards:

4.3.1. Minimum length: At least eight (8) characters when coupled with multi-factor authentication, otherwise at least ten (10) characters.

4.3.2. Complexity: Combination of uppercase and lowercase alpha and numeric characters and at least one special character (e.g., %, #, !).

4.3.3. The use of a passphrase, which is a string of four or more random, unrelated words strung together is recommended. When coupled with complexity requirements, this increases password strength.

4.3.4. The use of shared user accounts must be minimised. If shared accounts are used, passwords to these accounts must be shared securely and changed when staff with knowledge of the password leave the Foundation.

4.3.5. When end users receive passwords to user accounts the passwords must be shared securely.

4.3.6. IT systems in use at the Foundation, must allow for end users to select their own password or change their password at first login.

4.3.7. Default administrative passwords on devices must be changed.

4.3.8. When an account compromise has occurred or is suspected, passwords on these end user accounts must be changed.

4.3.9. To minimise password incrementation, passwords should be more complex and changed when required. Both examples below are secure passwords:

- Random characters: Hn8$lp&A
- Memorable passphrase, with altered characters: No1-CanGuessMe!

4.4 Multi-factor authentication

4.4.1. Something you know: Password/PIN

4.4.2. Something you have: Phone/Email/Certificate

4.4.3. Something you are (biometrics): Facial recognition/Fingerprint

4.4.4. Multi-Factor authentication (MFA) must be used for IT systems/applications in use at the Foundation that are internet-facing and hold sensitive information.

4.5 Access to Data and Networks

4.5.1. Users shall not access (or attempt to access), copy, alter or delete the files or data of any other User, whether stored on the organisation computer system or resident on the local memory;

4.5.2. Users shall not access, (or attempt to access) network, servers or other network devices in respect of which the User has no legitimate reason to access, whether the User has the logical access rights to do so or not;

4.5.3. Users should respect resources and system integrity controls. Hence, Users shall not develop or execute programs to infiltrate the systems, damage software or alter components of the system.

4.5.4. The above specifically includes, but is not limited to:

- Attempting to decode passwords or access protected information;
- Attempting to probe, circumvent or subvert system or network security measures; and
- Attempting to alter attribution of origin of a communication facility.

4.6 Surveillance or spying

4.6.1. No employees, or any information service provider may pry into the personal affairs of other Users without a legitimate purpose for accessing their files, data or communications.

4.6.2. Violation of 4.5.1 above will result to:

- Institution of disciplinary proceeding and depending on the transgression may result in termination of employment or summary dismissal;
- May exposed themselves personally to claims for damages for wrongful infringement of privacy rights; and
- May be liable to criminal prosecution.

4.7 External network security

4.7.1. Users shall not access, (or attempt to access) External networks, servers or other network devices in respect of which the User has no legitimate reason to access, whether the User has the logical access rights to do so or not.

4.7.2. If there is a need to establish a modem connection to any external network, SARGF will endeavor to ensure that access is provided and obtained.

4.7.3. Any computer devices or peripherals not connected to the SARGF network must be adequately protected against any forms of malicious codes such as viruses.

4.8 Access Rights Review

4.8.1 All user access rights shall be review bi-yearly by all business Unit Managers for all SARGF business applications which include and not limited to the following:

- Sage Evolution

- Banking System/Profile
- Document Management System
- Intranet/Shared Drive
- Database Applications

5. Authorised use and privacy

5.1 Use for legitimate business purposes only

a. The organisation's computer system is the property of SARGF, and it is intended to be utilized for organisational business. Only persons authorized by SARGF as "Users" may access the organisation computer and only to the extent that such access is required to assist them in the performance of their work. All Users shall use the organisation computer system in a professional, ethical and lawful manner.
b. Any User who is not permanently employed by SARGF shall enter into an agreement with SARGF governing the User's relationship with the organisation. This agreement shall incorporate the terms of this policy and provide for appropriate penalties against the User for any breach of his or her obligations set out in this policy; and
c. The appropriate line manager authorising access to any SARGF data or the SARGF computer system to a User not employed by SARGF shall ensure that the User has signed the appropriate agreement and such access has been approved by the Executive Director

5.2 Limited personal use permitted.

5.2.1. Incidental and occasional limited personal use of the organisation computer system is permitted, providing at all times that such use does not:
   a. Interfere with the User's work or performance;
   b. Interfere with any other User or employee's work or performance;
   c. Interfere unduly with the operation or resources of the SARGF computer system; or
   d. Violate any other provision of this policy or any other applicable policy, guideline or rule of the organisation.
   e. If the SARGF computer system is used to create, send, receive or private personal data, then in order to protect the privacy of any such data, the User must designate such data as private;
   f. The above provisions notwithstanding, Users expressly waive any right of privacy in anything they create, store, send or receive on the SARGF computer system, e-mail system, the internet or any other computer system;
   g. Users further consent to allowing SARGF when required, to access and review all material that the User has created, stored, sent or received on the organisation computer system or received through the internet or any other computer system as per the terms and conditions stated in this policy.
   h. Users should understand that SARGF may use human or automated means to monitor the use of its computer resources and the organisation computer system;
   i. SARGF acknowledges the privacy of data/folders identified as private, and

subject to the right of the organisation to access such data in terms of this policy and any other relevant legislation, it will refrain from doing so; and

j. Use of assigned usernames and the facility to choose passwords to gain access to the organisation computer system does not imply that Users should have an expectation of absolute privacy or confidentiality in the material they create and/or receive.

6. Computer usage

6.1 Physical security

6.1.1. It is the responsibility of every User to ensure that their personal computer and associated peripheral devices are adequately protected against theft and damage.

a. In the case of a laptop computer, the User must ensure that the supplied security cable (provided that one is supplied) is attached to the computer and secured to a desk or similar object or is stored in a locked cabinet outside of normal working hours or when left unattended;

b. In the case of a desktop computer and peripherals, the User must ensure, as far as possible, that the office in which the desktop computer is resident is adequately secured at the close of business or while unattended for any lengthy period of time; and

c. Mobile devices including portable computers of whatever nature, personal digital assistants, mobile telephones and peripherals devices must not be left unattended in motor vehicles or public places.

6.1.2. In the event of SARGF suffering any financial loss as a result of the User's failure to properly protect the security of any SARGF computer equipment (as mentioned above), the User may be held accountable for such loss;

6.1.3. Where a User wishes to temporarily remove computer equipment from any SARGF (except for Users allocated laptop computers), written authorisation is required from the Unit Manager.

6.1.4. In the event that authorisation is obtained in terms of 6.1.3 above, such equipment must be returned in the same condition and within the agreed time period;

6.1.5. Should IT equipment be stolen, it must be reported immediately to Police and the Finance and Administration Unit so that the appropriate steps can be taken, (for example, insurance claims and removal of logical access);

6.1.6. Users shall escort all visitors to the SARGF premises. Visitors to any SARGF premises must complete the visitors' register and be signed in by their host before entering the offices:

a. Users shall not permit visitors to gain access to restricted areas by allowing themselves or others to be followed through security doors and/or other mechanisms.

b. Users should always keep all access devices and security tokens under their personal control; and

c. Users are responsible for the consequences of permitting people to gain access to restricted areas and should challenge people without proper identification.

6.2 Logical Security

6.2.1. Users are responsible for ensuring the security, integrity and confidentiality of all data and information on the local memory of their personal computers.

6.2.2. In addition to the rules relating to passwords, Users shall take reasonable steps to ensure that no confidential material in the memory of their personal computer is –

a. Visible during their absence from their personal computer; or
b. Otherwise, accessible by unauthorised people.

6.2.3. Reasonable steps include the following:

a. Enabling the password facility on the approved screensaver program;
b. Enabling passwords to secure files containing confidential information; and
c. To the extent possible, not storing confidential material on laptop and desktop computers.

6.3 Saving and removing data

6.3.1. Users are strictly prohibited from saving and forwarding organisational information, data or files onto their portable computers, e-mail, disk, CD-ROM or any electronic or other storage media and removing it from the organisation premises other than in accordance with this clause.

6.3.2. Any User requiring access to organisation confidential information, data or files, whilst in any location other than at the organisation premises, shall obtain the express permission of the Executive Director or anyone acting in that capacity and will be subject to, inter alia, the following conditions:

a. The remote use of organisation confidential information, data or files may only be made by Users in the performance of their work functions for and on behalf of the SARGF;
b. The organisation confidential information, data or files will remain the property of the organisation at all times and Users will not acquire any right against it.
c. The User further undertakes to protect and safeguard the aforementioned confidential information, data or files, in a diligent and conscientious manner, and to perform a comprehensive virus scan where data or information has been used on a personal computer or other device not belonging to SARGF, prior to re-introducing data or information onto SARGF computer or computer system;
d. The User will promptly return the organisation's confidential information, data or files at the request of the organisation and/or destroy any copies thereof; and
e. This clause shall not limit any other right of the organisation with regard to its confidential information, data or files.

6.4 Computer system maintenance

6.4.1. The technical IT department shall carry out all maintenance and support of the organisation computer system and peripherals. Accordingly, Users may under no circumstances:

a. Attempt to repair their own personal computers, or those of other Users; or
b. Allow unauthorised technicians to provide any support, repair or maintenance on the organisation computer system.

6.4.2. Any failure to adhere to the provisions of 6.4.1. may not only result in disciplinary action pursuant to the provisions of this policy but may result in the User becoming personally liable to the organisation for any damage or loss suffered by the organisation as a result of his/her conduct.

6.4.3. Users must report all IT related requests for service to the Finance and Administration Unit, who will prioritise the call based upon its importance and allocate the IT contracted company to attend to such service call. Examples of such requests for service include but not limited to:

a. Suspected virus activity;
b. Theft of computer equipment;
c. Non-availability of network resources; and
d. Password resets.

6.5 Software usage

6.5.1. The organisation has licensed or developed certain software for use on the organisation computer system. The software is proprietary to SARGF and third parties. In order to protect its proprietary interests and to ensure compliance with the terms of applicable licenses, Users are expressly prohibited from –

a. Copying or granting software for use on any computer other than the SARGF supplied personal computer without the written permission of the Executive Director or information security personnel having the authority to grant such permission.
b. Copying or granting access to organisation software for distribution to independent contractors, clients or any third party.
c. Installing or downloading any software other than software onto the organisation's computer system.
d. Modifying, revising or adapting any organisation software.
e. Translating, reverse engineering or disassembling of any software resident on the organisation's computer system; and
f. Creating and installing software on the organisation's computer system without the prior written permission of the Executive Director

6.5.2. If at any stage a User believes that a particular software product, whether freeware, shareware or proprietary software, would assist in the furtherance of the organisation's business then a motivation should be sent to the Finance and Administration; and

6.5.3. Users are referred to of this policy for a list of software approved for use on the organisation computer system. These Annexures will be updated on a regular basis and published on SARGF Shared Drive from time to time.

6.6 Data storage and classification

Data created by Users on the computer system constitutes an asset of SARGF, and as such, all Users are required to classify data according to the guidelines below:

6.6.1 Sensitive information

a. Client-sensitive information is information relating to a client, which if disclosed to, or misused by unauthorised persons, could cause significant harm to the client and thus to the Organisation this information particularly information pertaining to the Treatment and Counseling clients should be used in accordance to the Protection of Personal Information Act (POPI).
b. Organisation-sensitive information is information relating to the organisation that, if disclosed to, or misused by, unauthorised people outside the organisation could cause damage or embarrassment to the organisation.

6.6.2 Unclassified internal information

a. Unclassified internal information is information that is to be regarded as "public" for internal use only and as a consequence requires lower level or security, since a breach would not damage the organisation or any of its clients.

6.6.3 Unclassified public information

a. Unclassified public information is information that is intended to be public and may be made available to any person outside the organisation after obtaining the appropriate permission.

6.6.4 Personal information

a. Personal information is information of a personal nature to the User and has no bearing whatsoever on the business activities of the organisation. Such information is prohibited from being stored on the organisation computer system other than in accordance with this policy.
b. Data classified as sensitive and personal information must be protected during transmission and storage (e.g. using password protection).

6.6.5 Virus Protection

6.6.5.1 Users are alerted to the fact that viruses can cause substantial harm to the organisation's computer systems. The damage caused is often not limited to hardware or software but can result in financial loss to the organisation as a result of lost production Therefore:

a. Users are to ensure that the latest SARGF-approved

antivirus protection software has been installed on their personal computer and is permanently enabled.

b. Should any data be received by a User through any other external source, a comprehensive scan of that data should be performed prior to loading that data onto the organisation computer system.
c. If a virus is detected, the Finance and Administration Unit should be notified immediately.
d. Installation of non-organisation approved virus protection software is prohibited.
e. Users are under no circumstances should anyone uninstall the anti-virus software or re-configure any settings on the anti-virus software unless specifically authorised by the Executive Director;
f. Users should never distribute virus information e.g. hoax virus e-mails (real or otherwise) to others. If any User encounters virus information, they should forward it to the Finance and Administration Unit.

6.6.6 Data encryption

The use of any form of cryptography on the organisation computer system in the transmission of any e- mail, storage of data or internet browsing is strictly prohibited. Where the nature of work requires it or the User needs to transmit sensitive information across entrusted networks, the User shall acquire a suitable data encryption program from the Finance and Administration Manager and shall place all private keys in compliance with directions given on the data encryption program.

Apart from usernames and passwords, Users may not use passwords or other encryption keys to prevent access to their e-mail on the organisation computer system.

6.6.7 Internet Usage

Users may be granted Internet access through the organisation's computer system, subject to approval by the respective Line Manager. Due to the nature of the Internet, it is essential that Users comply with the rules as set out below. Failure by Users to comply with these requirements relating to the use of the Internet could have serious financial and legal consequences for the organisation and may result in the personal liability of the User.

a. Users may not use Internet access provided by the organisation to conduct any other business other than that of the organisation.
b. Users may not use Internet access provided by the organisation to host or display personal web pages.
c. Users may not download any documents or images not related to organisation business or that have been specifically excluded unless expressly authorized by the direct line manager.

d. Users may not subscribe to or participate in chat groups, bulletin boards, newsgroups, or discussion groups that are not business related.
e. Users may not browse the internet for non-business purposes during organisation time.
f. Users may not post images or data which constitute prohibited material.
g. Unless specifically authorised by Managers, Users may not transact on behalf of SARGF via internet (i.e. purchase of goods or services), or submit corporate credit card numbers online.
h. Downloading of data via File Transfer Protocol websites is permitted provided that it is business related, and prior permission has been obtained from Finance and Administration Manager or his / her line Manager.
i. Users are prohibited from using or posting sensitive and personal information while accessing the Internet, (including but not limited to usernames, passwords, security codes or server-specific information) which could assist third parties in gaining unauthorised access to the SARGF computer system.
j. Users are prohibited from publishing or transmitting organisation data of a confidential nature on or via internet. If a situation exists where prohibited material has to be transmitted, written authorisation will be required from the Executive Director or person authorised by him/her, prior to the transmission or publication of such information on or via the internet. If such authorisation is conditional all conditions shall be met before transmitting the confidential material.
k. Users may not knowingly introduce viruses into the organisation computer system; and
l. Users are prohibited from accessing websites which contain prohibited material. Without derogating from this statement, SARGF may apply the use of filters (i.e. Websense) in respect of certain websites, which it deems to be undesirable (whether or not such websites contain prohibited material).

7. E-MAIL USAGE

7.1 Restrictions

The organisation e-mail system may not be used –

a. To initiate or forward any chain-message or other message which asks the recipient to forward such message to multiple other Users unless required for work purposes.
b. To send unsolicited commercial e-mail to people with whom the sender does not have a prior relationship.
c. To send frequent and / or numerous e-mail messages with the intention of disrupting or inconveniencing the receiver.
d. To send or forward any attachment listed in Annexure B; and

e. To send or forward any e-mail message, in the absence of written authority to the contrary, which in total, including any files or attachments thereto, exceeds 3MB in size.

7.2 Email Usage

a. The SARGF e-mail system may not be used for personal information dissemination or storage of personal advertisements, solicitations, promotions, destructive programs, political material, or any prohibited material.
b. The forwarding of e-mail messages without a legitimate business purpose, which is likely to lead to the embarrassment of the original sender, or in violation of the clearly expressed intention or request of the original sender to restrict further dissemination, is prohibited.

7.3 Prohibited material.

a. The use of the SARGF e-mail system to send, download, display or store prohibited material is prohibited.
b. No employee shall knowingly send or store any form of electronic communication containing prohibited material.
c. If any User is uncertain as to whether or not any material or statement constitutes prohibited material, such User must obtain clarification from the Finance and Administration Manager without delay; and
d. E-mail containing prohibited material which has been inadvertently received by a User shall be deleted as soon as he or she becomes aware of the content thereof and the incident must be reported to the Finance and Administration Manager or information security personnel authorized by him or her, without delay.
e. Users may not disguise their identity while using the SARGF e-mail system.
f. Users may not alter the 'From' line or any other indication of the origin of an e-mail message.

7.4 User obligations with regard to e-mail

7.4.1 Use of the disclaimer

The disclaimer will be automatically displayed on e-mail messages transmitted for and on behalf of SARGF. Users shall ensure the following:

a. Every e-mail message which is transmitted for and on behalf of the organisation contains the Disclaimer at the start of every such message.
b. Every business-related e-mail has the SARGF User defined signature which will consist of the following:
   (i) Name and Surname.
   (ii) Position the user holds.
   (iii) Direct line.
   (iv) Fax Number.
   (v) E-mail address; and
   (vi) SARGF's website address

c. No personal e-mail contains any User-generated indication that it is from or has the sanction of SARGF; and
d. In order to indicate the privacy of any particular e-mail communication, the User shall designate any such communication as "private" and store it in a folder identified as such.

7.4.2 Formal correspondence and other documents

a. Any formal document of SARGF, which any User wishes to transmit via e-mail, shall be sent as an attachment to an e-mail message, on the organisation letterhead template provided for this purpose or other formal correspondence material.
b. Users are alerted to the fact that e-mail communications can bind SARGF to an agreement and as such the Users need to comply with the relevant organisation policies as communicated to them in this regard. If the User is in any doubt, clarification should be obtained from the Finance and Administration Manager; and
c. All e-mail communications are SARGF records. The organisation reserves the right in its discretion to access and disclose all legitimate business communications sent using the SARGF e-mail system.

7.5 Transmission of organisation information by means of e-mail

7.5.1 Users of the organisation e-mail system shall respect the organisation's proprietary interest in its confidential material.

7.5.2 Confidential material shall not be sent, transmitted or otherwise disseminated by Users to third parties unless the User has satisfied himself / herself that:

a. He / She is duly authorised to send, transmit or otherwise disseminate the relevant confidential material;
b. It is in the ordinary course of the business of the organisation or in the organisation's best interests to the send, transmit or otherwise disseminate such confidential material; and that
c. Such confidential material is already in the public domain; or
d. The intended recipient is confidential and is entitled to receive such confidential information of material.

7.5.3 Only confidential material that complies with the requirements of the above may sent via the organisation e-mail system.

7.5.4 Personal data concerning any employee or any third party as may be kept as part of SARGF records shall not be disclosed to anyone without the prior authorisation of the employee or third party concerned. Prior written authorisation of the relevant Unit Manager together with directions as to the manner in which such records may be disclosed is also required.

7.6 Attorney-client communication by e-mail

7.6.1. All communications, including e-mails communications, between the organisation and its legal representatives may be privileged and all such messages:

a. Shall be suitably and prominently identified as such therein; and
b. May not be disclosed to anyone else without the prior authorisation of the Executive Director serving the organisation premises, or someone to whom they have delegated this authority in writing.
c. Such e-mail shall not be divulged to employees of SARGF if they were not a party to the e-mail communication in question.

7.6.2. Exceptions

a. If it is not possible to send such an e-mail using the organisation computer system, then such e-mail should be sent via the Internet in an encrypted format authorized and approved by the Finance and Administration Manager.

7.7 Retention of data including e-mail

In the same way as printed documents, correspondence and material is subject to retention policies, as is the data and e-mail belonging to SARGF.

7.7.1. Users are required to ensure that all data that may be required to be retained in terms of applicable regulations or in terms of SARGF's document retention policies as communicated to them are retained and sorted in compliance with such legislation or such policies.

7.7.2. If a User is uncertain as to how to effect the retention of any data, he or she shall refer to obtain instruction from the Finance and Administration Manager.

7.8 Disclosure of data contained in e-mail

No User shall of his or her own accord, under any circumstances, respond in any way to a discovery notice or demand to disclose any particulars with regard to SARGF, e-mail or to any subpoena to produce an e-mail at any court proceedings, (other than to acknowledge receipt thereof if necessary) without first obtaining the authority and advice of the Executive Director or someone authorized by him or her in writing.

7.9 Monitoring

7.9.1 The SARGF computer system is provided to Users, at SARGF's expenses, for use in the promotion of organisation business and incidentally for personal purpose. In order to protect its rights and interests, SARGF will routinely monitor all internet usage and e-mail traffic on the organisation e-mail system.

7.9.2 The application is designed to alert the Finance and Administration Manager to any prohibited use of the SARGF e-mail system and additionally identify forbidden words, strategic phrases relating to strategic projects and confidential material / files of SARGF.

7.9.3 While all e-mail will not be routinely read, those e-mails identified by the software as potentially infringing this policy, may be accessed at the discretion of SARGF by anyone authorised to do so.

7.9.4 SARGF reserves the right to access and read the contents of e-mails messages and track internet usage in the following circumstances:

a. Insofar as it is required by law or legal obligations to third parties to do so;
b. If there is a legitimate business need or reason to do so (e.g. when traffic monitoring is not sufficient to establish violation of this policy or any relevant legislation);
c. In order to protect the SARGF's interests in the event that it reasonably suspects that a User has committed or is committing a crime that might be aimed at the organisation, or in respect of which the organisation may incur any liability, whether criminal or financial; and
d. If it is of the bona fide opinion that such access or disclosure may be necessary to investigate a breach of the security of the email system or this policy.

7.9.5 Provided that, subject to the restrictions set out below, SARGF will not seek access to the contents of any User's e-mail files without the permission of the User concerned.

a. Should the Finance and Administration Manager encounter indications of illegal activity or violations of organisation policy or security, the Finance and Administration Manager, or information security personnel authorized by him or her shall investigate further and report any findings to the head of the department concerned;
b. Users must ensure that all business-related e-mail messages that should be available to other Users should be made available on a need-to-know basis; and
c. The User consents to access the organisation to protect the organisation's computer system and data or the organisation's proprietary rights.

7.10 Disclosure

7.10.1 Internal Disclosure

The contents of legitimate business e-mail may be disclosed within the organisation without the permission of any User who was the addressor or addressee of such e-mail. However, any internal disclosure within the organisation without the consent of the Users concerned shall be limited to those Users or employees who have a reasonable need for access to such e-mail.

7.10.2 External Disclosure

a. SARGF may in its discretion and for any legitimate purpose, disclose to third parties the contents of e- mail messages sent to, or received by its Users.

b. The organisation will, however, attempt to accommodate any objections to such disclosure on the following grounds, reasonably based:

(i) That such disclosure will create personal embarrassment for the User concerned, unless such disclosure, in the organisation's discretion, is required to serve an important business purpose or satisfy a legal obligation; or

(ii) That the contents of such message are personal and private in nature and the organisation is not under way legal obligation to make such disclosure.

7.11 General Terms

7.11.1 Use of information for bona fide business purposes

a. The organisation may use data regarding the number, sender, recipient and addressees of e-mail communications sent over the organisation e-mail system for any bona fide business purpose provided that in so doing it will not contravene any data protection legislation applicable to the country from which the e-mail was sent or received.

7.11.2 Legal obligation to disclose

a. If the organisation is legally obliged to disclose e-mail messages to third party, the organisation shall give reasonable prior notice to the User whose e-mail is required to disclosed, unless:

(i) The organisation is legally obliged to allow such disclosure without such reasonable notice or without any notice at all; or

(ii) Such disclosure is required by law enforcement agency; and

(iii) It is contrary to the interests of justice or law enforcement to notify the User of such disclosure; or

(iv) The organisation has prima facie reason to believe that the law enforcement activity relates to the possibility that the organisation may be the victim of a crime.

7.11.3 Any request made to the organisation for access to the contents of e-mail without consent or knowledge of the sender or recipient shall be considered by the head of the department concerned on the condition that:

a. Such requests must be approved in advance. Any access without such approval shall constitute a breach of this policy; and

b. The use or disclosure of data obtained from inspection or monitoring of organisation e-mail must be reviewed and approved in advance in writing by the Unit Manager concerned.

7.11.4 Unauthorised use to be reported

a. Users shall not knowingly permit the unauthorised use of the organisation e-mail system. Any unauthorised use of the organisation's e-mail system must be reported without delay to the Unit Manager in which unauthorised use occurred, and to the Finance and Administration Manager without delay.

7.11.5 Consequences and violation

a. The terms and conditions of this policy have the force and effect of the organisation rules;
b. Penalties for contraventions of this policy may expose the User to disciplinary action in accordance with the SARGF's disciplinary code as amended from time to time; and
c. Management reserves the right to discipline offenders in terms of this policy.
d. A User who contravenes the terms and conditions of this policy acknowledges that he or she will be acting outside the course and scope of his or her employment, or his or her contractual obligations to the organisation. With regard to a non-employee User of the SARGF computer system such User shall be obliged to enter into a written agreement with the SARGF that shall expressly prohibit any contravention of this policy.

8 Privacy and confidentiality

a. Due care must be taken with the secure use, storage and sharing of personal information held by the Foundation. Such information must be collected, processed, stored and transferred among the Foundation and third parties, only in a manner that is consistent with the Foundation's business practices and policies, and in compliance with the Protection of Personal Information Act 4 of 2013 (POPIA) and the Foundation's Promotion of Access to Information Act (PAIA) Manual.

9 Compliance with law and policy

a. The Foundation's IT infrastructure and facilities may only be used for authorised purposes. The Foundation may from time-to-time monitor or investigate usage of IT facilities and any person found using IT facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary and, where appropriate, legal proceedings. Furthermore, the Foundation shall only permit the inspection and monitoring of operational logs by computer operations personnel and system administrators. Disclosure of information from such logs, to officers of the law or to support disciplinary proceedings, shall only occur when required by and consistent with law, there is reason to believe that a violation of law or of an institution policy has taken place, or there are compelling circumstances.

b. To ensure that all software and licensed products used within the Foundation comply with the requirements of various acts relating to copyright, designs and patents, the

Foundation will carry out checks from time to time to ensure that only authorised products are being used, and will keep a record of the results of those audits. Unauthorised copying of software or use of unauthorised products by staff may be grounds for disciplinary and, where appropriate, legal proceedings.

c. It is unacceptable for anyone to use information resources to violate any law or the Foundation's policies or perform unethical business acts. In this regard, the reader is referred to the Code of Conduct for Employees.

10 Regular Backups

a. Regular backups of central information stores that are considered high value (i.e. if lost or unrecoverable for an extended period of time, would impact on the operations of the organisation) must be performed.
b. The backup must be stored in a different location to the original data that is backed up.
c. Backups must be scheduled according to the availability and integrity requirements of the information that is being backed up. A backup schedule must be documented and maintained for the Foundation 's critical information systems.
d. A simple data recovery test for important IT systems must be performed annually.

11 Patch Management

Patch management processes must be undertaken centrally with reporting on patch status provided.

A formal patch management process using a patch management tool is documented, maintained and followed to:

Identify and assign vulnerability resolution ownership.

- Rate vulnerability criticality.
- Determine management response (plan of action) timeframes.
- Determine vulnerability resolution timeframes.
- The process for applying security patches must provide for timely identification, assessment and installation of patches in response to recognised vulnerabilities.

Operating System and application security patches must be applied in accordance with the severity of the vulnerability. When determining the criticality of vulnerabilities and patches, the following must be considered:

- Industry recognised rating schemes such as CVSS (Common Vulnerability Scoring System);
- Vendor-supplied patch classifications and recommended resolution timeframes;
- The organisational context-specific assessment of criticality, sensitivity, threats of/to the affected service or software.

All patches applied in the the Foundation environment must be obtained from reliable sources and verified using available mechanisms, such as cryptographic checksums.

Security patches must be adequately tested prior to application to production systems to ensure service availability is maintained.

Configure Microsoft Office macro settings

Only specific Microsoft Office applications for which there is a demonstrated business requirement for macro use should be allowed to execute approved macros from trusted locations or macros that are digitally signed by trusted publishers. All other Microsoft Office applications should have support for macros disabled.

12 Security incidents reporting and management

a. All users have the responsibility to report immediately to the IT Department, by telephone at 011 026 7323 or via the following link https://responsiblegambling.org.za/incident-report/ any observed or suspected security incidents where a breach of the Foundation's security policies has occurred, and any security weaknesses in, or threats to, systems or services. This is required not only to prevent and resolve incidents, but also for the institution's responsibility to report certain security breaches in compliance with the POPIA and the Cybercrimes Act.

13 IT Department is responsible to:

a. implement mechanisms to detect, report and analyse IT security incidents.
b. implement and maintain incident management procedures to ensure a rapid and consistent response to incidents; and
c. analyse incidents to mitigate the risk of future incidents and improve the incident management procedure.