AfriForum Information Security Policy

Internal and External Information

Internal Sources Files and Client Information

Document Name: AfriForum Information Security Policy
Last Updated Date: 24 April 2021
Version: 1.4

Disclaimer

This policy, its attachments, and any rights attaching hereto are, unless the context clearly indicates otherwise, the property of AfriForum. It is confidential, private and intended for the addressee only, and may only be used by the addressee for the particular purpose for which the policy has been requested. The addressee shall furthermore treat all personal information that comes to its knowledge or into its possession as confidential and shall not disclose it without the consent of AfriForum.

AfriForum accepts no liability whatsoever for any loss or damages, whatsoever and howsoever incurred or suffered, resulting or arising from the use of the information in the policy or its attachments.

Table of Contents

1. Introduction

1.1. AfriForum: Information Security Policy

The AfriForum information security policy addresses all levels of information and systems security applied within the company. The policy addresses all internal information, documentation and data as well as all client data stored within the company's databases or the companies' suppliers' databases.

1.2. The Purpose

This Information Security Policy document is aimed to define the security requirements for the proper and secure use and storage of the Information Technology services in the company. Its goal is to protect the company its clients and members to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation, and business outcomes.

1.3. The Scope of the Information Security Policy

This document applies to all the employees in the company, including temporary employees, visitors with temporary access to services and partners with limited or unlimited access to, company, members, employee and/or vendors information. Compliance with policies in this document is mandatory for this constituency.

1.4. Document History

Version	Description	From	Author
1.4	Initial version	2021/04/24	Nic Pieterse
	Revision and Changes		
	Revision and Changes		
	Revision and Changes		
	Revision		

2. Responsibilities

Roles	Responsibilities
Information Security Officer	• Accountable for all aspects of the companies and member information security.
Information Security Officer	• Responsible for the security of the IT infrastructure. • Plan against security threats, vulnerabilities, and risks. • Implement and maintain Security Policy documents. • Ensure security training programs. • Ensure IT infrastructure supports Security Policies. • Respond to information security incidents. • Help in disaster recovery plans.
Information Owners	• Help with the security requirements for their specific area.

	• Determine the privileges and access rights to the resources within their areas.
IT Security Team	• Implements and operates IT security. • Implements the privileges and access rights to the resources. • Supports Security Policies.
Employees	• Meet Security Policies. • Report any attempted security breaches.

3. General Policy Definitions

- Exceptions to this policy defined in any part of this document may only be authorized by the Information Security Officer. In those cases, specific procedures may be put in place to handle request and authorization for exceptions.
- Every time a policy exception is invoked, an entry must be made into a security log specifying the date and time, description, reason for the exception and how the risk was managed.
- All the IT services should be used in compliance with the technical and security requirements defined in the design of the services.
- Breach of this policy may lead to disciplinary actions. In some serious cases they could even lead to prosecution.

4. IT Assets

This section of the Information Security Policy describes the details for the secure handling of the IT assets of the Company.

4.1 Purpose

The IT Assets section defines the requirements for the proper and secure handling of all the IT assets in the Company.

4.2 Scope

This section of the policy is aimed at permanent employees and sub-contractors that use IT equipment allocated to them to perform their day-to-day tasks as well as ad hoc task that might need to be performed on a project-by-project basis.

The policy applies to desktops, laptops, data modems, screen projectors, audio and video equipment and other equipment involved in the provision of the IT services.

4.3 Definitions

- IT assets must only be used in connection with the business activities they are assigned and / or authorized.
- Every user is responsible for the preservation and correct use of the IT assets they have been assigned.
- All the IT assets must be in secure and safe environment in the care of the allocated user.
- Active desktop and laptops must be secured if left unattended.
- Access to assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provision of a service must be done through the approved by the direct Line Manager.
- All personnel interacting with the IT assets must have the proper training.

- Employees shall maintain the assets assigned to them clean and free of accidents or improper use. They shall not drink or eat near the equipment.
- Special care must be taken for protecting laptops and other portable assets from being stolen.
- When travelling by plane, portable equipment like laptops and data modems must remain in possession of the user as hand luggage.
- Losses, theft, damages of company assets must be reported as soon as possible to your Line Manager.
- Assets storing sensitive information must be completely erased in the presence of Line Manager before disposing.

5. Access Control

This section of the Information Security Policy describes the details for securing Access Control.

5.1 Purpose

The Access Control section defines the requirements for the proper and secure control of access to IT services and infrastructure in the Company.

5.2 Scope

This section of the policy applies to all the employees in the Company, including temporary employees or contractors, visitors with temporary access to services and partners with limited or unlimited access time to services.

5.3 Definitions

- Any system that handles valuable information must be protected with a password-based access control system.
- Access to resources should be granted on a per-group basis rather than on a per-user basis.
- Access shall be granted under the principle of “less privilege”, i.e., each identity should receive the minimum rights and access to resources needed for them to be able to successfully perform their business functions.
- Whenever possible, access should be granted to centrally defined and centrally managed identities.
- Employees should refrain from trying to tamper or evade the access control to gain greater access than they are assigned.

6. Password Control

This section of the Information Security Policy describes the details for securing password control.

6.1 Purpose

The Password Control section defines the requirements for the proper and secure handling of passwords in the Company.

6.2 Scope

This section of the policy applies to all the employees in the company, including temporary employees, contractors, and visitors with temporary access to services and partners with limited or unlimited access time to services.

6.3 Definitions

- Any system that handles valuable information must be protected with a password-based access control system.
- Every user must have a separate, private identity for accessing IT network services.
- Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged through the O365 authentication solution Active Directory Services (AD).
- Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least 6 characters long.
- Password for some special identities will not expire. In those cases, password must be at least 6 characters long.
- Sharing of passwords is forbidden.
- Whenever a password is deemed compromised, it must be changed immediately.
- For critical applications, digital certificates and multiple factor authentication using smart cards, SMS or email should be used whenever possible.

7. Email

This section of the Information Security Policy describes the details for the secure handling of electronic mail.

7.1 Purpose

The Email section defines the requirements for the proper and secure use of electronic mail in the Company.

7.2 Scope

This section of the policy applies to all the employees in the company, including temporary employees, contractors, and visitors with temporary access to services and partners with limited or unlimited access time to services.

7.3 Definitions

All the assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of the company. Occasional use of personal email address on the Internet for personal purpose may be permitted if in doing so there is no perceptible consumption in the company system resources and the productivity of the work is not affected.

Use of the company resources for non-authorized advertising, external business, spam, political campaigns, and other uses unrelated to the company business is strictly forbidden.
In no way may the email resources be used to reveal confidential or sensitive information from the Company outside the authorized recipients for this information.

Using the email resources of the company for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is absolutely discouraged.

Use of the company email resources is maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the company, the associated account must be deactivated according to established procedures for the lifecycle of the accounts. Outbound messages from company employees should have approved signatures at the foot of the message.

Scanning technologies for virus and malware must be in place in user computer equipment to ensure the maximum protection in the ingoing and outgoing email.

8. Internet Policy

This section of the Information Security Policy describes the details for the secure access to the Internet.

8.1 Purpose

The Internet section defines the requirements for the proper and secure access to the Internet.

8.2 Scope

This section of the policy applies to all the employees in the company, including temporary employees, contractors and visitors with temporary access to services and partners with limited or unlimited access time to services.

8.3 Definitions

- Access to pornographic sites, hacking sites, and other risky sites is strongly discouraged.
- In accessing the Internet, employees must behave in a way compatible with AfriForum core values of the company. Attacks like denial of service, spam, fishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.

9. Antivirus Policy

This section of the Information Security Policy describes the details for the implementation of anti-virus and other forms of protection.

9.1 Purpose

The Antivirus section defines the requirements for the proper implementation of antivirus and other forms of protection in the company.

9.2 Scope

This section of the policy applies to Notebooks and PC workstations.

9.3 Definitions

- All Notebooks and PC workstations must have an antivirus client installed, with real-time protection.
- All the installed antivirus protection software must automatically update their virus definition. They must be monitored to ensure successful updating is taken place.

10. Information Classification, Safeguarding and Destruction

This section of the Information Security Policy describes the details for the classification and use of information.

10.1 Purpose

The Information Classification section defines a framework for the classification of the information. It is aimed at ensuring the appropriate integrity, confidentiality, and availability of the company information.

10.2 Scope

This section of the policy applies to all the information created, owned, or managed by the company.

10.3 Definitions

- Employees must ensure the security of their information and the systems.
- Each employee is responsible for ensuring the confidentiality, integrity and availability of the Company's assets, information, data, and IT services.
- Information in the company is classified according to its security impact. The current categories are confidential, shareable, and public.
- Information defined as confidential has the highest level of security. Only a limited number of persons must have access to it. Management, access, and responsibilities for confidential information must be handled with special procedures defined by Management and personal information of employees, members, and juristic persons in accordance with the POPI act.
- Information defined as shareable can be shared outside of the limits of the company, for those clients, Companies, regulators, etc. who acquire or should get access to it.
- Information defined as public can be shared as public records, e.g., content published in the company's public Web Site and Portal Sites.
- Information is classified jointly by the employees and Management and in accordance with the south African POPI Act for handling personal information of employees, members, and juristic persons.
- All personal information of employees, members and juristic persons must be saved within the companies **provisioned data basis** by all employees in the company, including temporary employees, contractors, and visitors with temporary access to services and partners with limited or unlimited access time to services.
- All employees in the company, including temporary employees, contractors, and visitors with temporary access to services and partners with limited or unlimited access time to services must familiarize themselves and comply to the company's "Clean Desk Policy" on information security and safeguarding.
- Data destruction, deletion and or shedding of paper documentation holding personal information of employees, members and or juristic persons may only be done with the approval of the companies Information Officer or designated Deputy Officers.
- Requesting of destruction, deletion of data on the company's data basis or the shredding of paper documents containing personal information, must follow the formal process whereby employees, members or juristic persons complete the form "**Request for Destruction, Deletion or Shredding**" and obtain the approval of the respected Information Officer.
- Data Subjects might also request for the destruction, deletion, or the shredding of their personal information. This request must also follow the same process as described above whereby the Data Subject needs to fill out the "**Request for Destruction, Deletion or Shredding**" form and obtain the approval of the respected Information Officer.

11. Annex A

11.1 Glossary

Term	Definition
Access Management	The process responsible for allowing employees to make use of IT services, data, or other assets.
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.
Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Confidentiality	A security principle that requires that data should only be accessed by authorized people.
External Service Provider	An IT service provider that is part of a different Company from its customer or called a third-party operator
Identity	A unique name that is used to identify an employee, person, or role.
Information Security Policy	The policy that governs the Company's approach to information security management
Outsourcing	Using an external service provider to manage IT or data processing services.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure etc.
Risk	A possible event that could cause harm or loss or affect the ability to achieve objectives.
Service Level	Measured and reported achievement against one or more service level targets.
Warranty	Assurance that a product or service will meet agreed requirements.
Destruction of Data	The process of destroying data stored on tapes, hard disks, and other forms of electronic media so that it is completely unreadable and cannot be accessed or used for unauthorized purposes.
Deletion of Data	Data Deletion is a software-based method of overwriting the data that aims to completely destroy all electronic data residing on a hard disk drive or other digital media by using zeros and ones to overwrite data onto all sectors of the device.
Shredding of Paper	To cut or tear into shreds.

Table 1. Glossary

Signed: _____ Date: _____

AfriForum Information Officer