RETINA SOUTH AFRICA (NPO 003-184)
eMail: headoffice@retinasa.org.za
Postnet Suite 75, Private Bag X10020, Edenvale 1610
Tel: 0860595959 Fax: 0866 536392

PIS-015 INFORMATION SECURITY POLICY

Table of Contents

Please read this policy because it applies to you.

Security

Retina South Africa (non-profit organisation) takes security very seriously, do our best to comply with applicable data protection laws and take all reasonable and appropriate measures to keep your personal information secure. For example, we encrypt our desktops, laptops, secure servers, firewall and server configuration. Mobile phones have built-in encryption through a PIN, password or facial recognition. However, we cannot guarantee the absolute security of it.

We back-up all your personal information on a regular basis.

Our hosting company hosts our website in a secure server environment that uses a firewall and other advanced security measures to prevent interference or access from outside intruders. We authorize access to personal information only for those employees who require it to fulfil their job responsibilities. We implement disaster recover procedures where appropriate.

This is our plan of action for safeguarding our website and your personal information from harm. It describes our responsibilities, our disclaimers and your responsibilities.

Our responsibilities

- Your personally identifiable information is stored by us and is maintained in a highly secure environment that uses a firewall and other security measures to prevent unauthorized access, is not available to the general public, which includes, but is not limited to, Internet and physical security, and is subject to strict managerial policies and procedures.

- We ensure that links from our systems to systems under the control of third parties are secure.
- protect your information that we store in or passes through our systems using encryption or other appropriate information security measures.
- ensure that links from our systems to systems that third parties' control are secure.
- backup all data on our systems so that we can recover it in case of disaster.
- log all access to our systems to better identify and resolve unauthorised access issues.

Your responsibilities

You may not do (or let anyone else do) anything that might **compromise** our system.

Recommended steps. You should take the following steps to secure your personal information:

- install security software on your device, including anti-virus, anti-spyware, and anti-spam software.
- regularly scan your device for viruses and other malicious software.
- keep security software up-to-date to ensure you are always running the latest version with the latest definitions.

Additional steps. You could take the following steps for your own security:

- check your Internet browser's security settings for ways to make your browsing more secure.
- make sure that you have entered secure pages when filling in your personal information.
- log out after you have transacted electronically.

Our Disclaimers

Disclaimer. We will do our best to prevent our website and your information from being compromised and will help you resolve a security problem whenever we can. However, we are not responsible for compromises caused by:

- harmful code entering our website, such as viruses, bugs, Trojan horses, spyware, or adware.
- your fault – problems or loss caused by your information you provide to us (such as inaccurate personal information) or your computer being compromised (such as being accessed by an unauthorised person or otherwise hacked).
- factors beyond human control – such as fires, floods, or other natural disasters.

Third party systems. Third parties are responsible for the security of information collected by, stored on, or passing through their systems, even if we link to those systems.

Phishing

Awareness. Be aware of ‘phishing’ attacks where criminals attempt to get your personal information by sending you an email, masquerading as an email from us, asking you to access your account or verify information through links in the email, or diverting you to a fake version of our website.

Legitimate URL. You must only log into our website from a legitimate URL associated with us that you know and trust, such as one based on our name that we have communicated to you in writing. Please be wary of phishing websites that use illegitimate URLs designed to trick you into thinking they are our website, such as by using common misspellings of our name, different domain suffixes, or other words associated with our business.

Reporting. Please report any suspected phishing attacks to us immediately to prevent any harm to you or others.

Acceptance and changes to terms of this policy

By accessing this website, submitting an enquiry, making a donation or subscribing to our newsletter, you are deemed to have read, understood, accepted, and agreed to be bound by the terms of this policy.

We may change the terms of this policy at any time without notification to you. Please be sure to check this Policy periodically for changes. If you do not agree with the changes, then you must stop using the website. If you continue to use the website the changed terms will apply to you and you will be deemed to have accepted those updated terms.

Enquiries

We welcome your feedback.

If you have any questions or concerns arising from this privacy policy or the way in which we handle personal information, please contact us.

Revision History

The policy (and the procedures, standards and guidelines supporting the policy) is reviewed by the Retina South Africa Management Committee regularly, and at least once in each year.

Reviews and any revisions of the policy (and the procedures, standards and guidelines supporting the policy) will be recorded in a Revision History filed with this policy.

Compliance with this policy (and the procedures, standards and guidelines supporting the policy) is monitored and may be subject to audit.

*** END OF POLICY ***

REVISION HISTORY			
Document Type	**Policy**		
Document Number	**PIS-015**		
Effective Date	**8 December 2021**		
Revision Details	**Rev No.**	**Date**	**Approver**
Origination of policy for committee approval	1	2021/10/26	MC
Ratification by MC	2	2021/12/08	MC