ANNEXURE "I" TO THE ASISA POLICY ON STATISTICS

CYBER STATISTICS

1 BACKGROUND AND PURPOSES OF STATISTICAL ACTIVITY

1.1 The rapid pace of change arising from an increasingly digital economy – alongside the growing industrialisation and increasingly borderless nature of the cybercrime industry – has resulted in one of the most pervasive and pressing challenges businesses face today. The financial sector faces significant exposure to cyber risk given that it is information technology-intensive and highly interconnected through payment systems. Cyber-attacks can pose a major impact on financial institutions, potentially compromising their sustainability.

1.2 Recognising the scale of the challenge, ASISA and SAIA established a joint Cyber Security Incident Response Team ("**CSIRT**") with a mandate to represent ASISA and SAIA members at an industry level in interactions with the SA Government and Regulators on issues relating to cyber security, share emerging cyber threats impacting the insurance and investment industry in South Africa, contribute towards the improvement of skills in SA to combat cybercrime and cyber security and address sector-wide issues in a collaborative setting.

1.3 In this context, the purposes of the cyber statistical activities set out in this **Annexure "I"** include:

1.3.1 assisting ASISA and SAIA members to fully understand the extent and intensification of cyber risks in the industry and to provide insight into emerging cyber threats, trends and issues;

1.3.2 using data analytics to develop indicators to measure current states of cybercrime;

1.3.3 providing collated cyber intelligence to ASISA and SAIA members to assist them to combat threats to cybersecurity and to improve cyber defence and resilience;

1.3.4 providing collated cyber statistics to regulatory authorities on request;

1.3.5 developing a standardized approach, for ASISA and SAIA members for collecting and reporting on cybercrime statistics aligned with pending regulation in the form of the draft Joint PA and FSCA Standard on Cybersecurity and Cyber Resilience and the Cyber Crimes and Cyber Security Bill and the Cyber Security Hub mandated by South Africa's National Cybersecurity Policy Framework;

1.3.6 developing consistent definitions to increase the accuracy and value of cyber statistics.

1.4 It is specifically recorded that this **Annexure "I"** does not intend to set out ASISA's and SAIA's respective expectations or guidelines in terms of the systems and controls their members should have in place to combat cybercrime or comply with relevant regulatory requirements. Each member must establish the security risk-management roles and decision-making processes that are appropriate for the particular member.

2 PARTICIPATING MEMBERS

2.1 All ASISA members may choose to participate.

2.2 In view thereof that CSIRT is a collaborative effort between ASISA and SAIA, the CEO has approved the participation by SAIA members on a voluntary basis. As such SAIA members may also choose to participate. Any reference in this **Annexure "I"** to Participating Member accordingly includes participating members of SAIA.

2.3 Information provided by Participating Members may be reported at a group level, i.e. across different license categories within the Participating Members' group of companies.

3 PROCESS

3.1 Participating Members must submit the required data in the required format to ASISA's Third Party Service Provider on a monthly basis by the 8th Business Day of the month.

3.2 ASISA's Third-Party Service Provider will collect and collate the Individual-Level Data and generate Collated Statistics.

4 STATISTICS

4.1 The following cyber security related information will be collected from Participating Members:

4.1.1 incidents – time, date;

4.1.2 number of incidents;

4.1.3 category (table);

4.1.4 impact – internal, external, both or none;

4.1.5 number of end points.

4.2 The incident categories are as follows:

Incident category	Description	Reporting guideline
Denial-of-Service **(DOS)**	Availability of certain services or components is impacted, through malicious actions.	
Compromised Information **(CIN)**	Personal information of individuals or intellectual property of the company leaked or attempted to leak it to external parties. OR attempted or successful destruction or corruption of company information	
Compromised Asset **(CAS)**	Compromised host (admin or root account, Trojan, rootkit); network device, application, user account. This includes passwords that were stolen or malware infections where control was taken of the device.	
Unlawful activity **(UAC)**	Theft/Fraud/Human Safety/ Child pornography – incident must be reported to Law enforcement	
Internal Hacking **(IHA)**	Reconnaissance or Suspicious activity originating inside the member network (excludes malware that shows similar behaviour)	

External Hacking **(EHA)**	Reconnaissance or Suspicious activity originating outside the member network (excludes malware)	
Malware **(MAL)**	A virus, worm or script typically affecting multiple corporate devices. This excludes hosts that are actively controlled by the attacker via a backdoor or a trojan. They will include ransomware.	A failure in existing anti-virus or malware control that requires action, investigation and correlation. These actions can be either automated or manual. These events are not business as usual events.
Phishing and Social Engineering **(PSE)**	Threat actors use email spoofing and voice communication to lure victims into performing actions that will compromise sensitive information or perform un-approved financial transactions.	A failure in the standard email protection or phishing mechanisms which cause sufficient impact or concern to warrant further investigation. These failures could be blocked by other security layers and constitute a control failure.
Third Party Compromise **(TPC)**	A party that is not a part of the reporting entity but is connected contractually or operationally. Examples are clients, service providers or vendors.	Compromise of third parties is reportable when the compromise is: a) known to the reporting entity. b) material in terms of effects on the relationship between the reporting entity and the third party c) material in financial terms to either the reporting entity, the third party or both

		d) significant in terms of data exposure e) significant in terms of contribution to a pattern Should a reporting entity be bound by a non-disclosure agreement, this should be honored and as much information regarding the compromise consistent with the NDA should be reported. When in doubt, the compromise should be reported, using the Chatham house rule.

5 COLLATED STATISTICS

The Collated Statistics will be incorporated into a quarterly ASISA Cybersecurity Status Report ("**Status Report**").

6 SHARING AND PUBLICATION

6.1 The Status Report will be shared with members of the CSIRT and the Technical and Operations Board Committee.

6.2 It is recorded that the CEO has, after due consideration, agreed that that the provisions in the Standard insofar as publication and dissemination of Collated Statistics may be deviated from in respect of the cyber statistics dealt with in this Annexure on the basis that there are justifiable reasons for doing so and such deviation does not pose a risk to contravention of the ASISA Competition Policy or competition laws.

DOCUMENT HISTORY

Date	First publication / amendment
31 July 2023	First publication.

RESPONSIBLE SPA AND COMMITTEES

Responsible Senior Policy Advisor	ASISA Point Person to the Technical and Operations Board Committee
Responsible Board Committee	Technical and Operations Board Committee
Responsible Standing Committee	CSIRT