DATA BREACH POLICY

BACKGROUND

This Data Breach Policy applies to the following legal entities :

1.1.1 West African International (Pty) Ltd (1995/008104/07); and

1.1.2 WAG Chemicals (Pty) Ltd (1986/003393/07**)**

(hereafter "we, "us" "the Company")

In terms the **Protection of Personal Information Act, 14 of 2013** (POPIA), where there are **reasonable grounds** to believe that the Personal Information belonging to a person or legal entity (Data Subject) has been accessed or acquired by any unauthorised person, *to wit* "data breach", the Company, as the Responsible Party, must notify the Information Regulator and the Data Subject of such breach, unless the identity of such Data Subject cannot be established.

This notification must be in writing and must provide the Data Subject with sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise.

This Data Breach Policy ("Policy") sets out how The Company and its Personnel will deal with a data breaches. A set of definitions as referred to in POPIA, to assist in the interpretations of this policy appear in the POPIA Manual of The Company, which should be read in connection with this Policy.

EXAMPLES OF INCIDENTS WHICH COULD GIVE RISE TO DATA BREACH

Security event	**Description of security event for clarification**
External Breach	Defined as a breach where unauthorised individual/s gain access to the internal network of The Company to steal, copy, modify and/or delete personal information from outside the organisation. This type of breach can be performed by utilising sophisticated cyber-attacks or simple attacks such as a successful phishing email.
Internal Breach	Defined as a breach where through an act of bad faith or malice an The Company employee/s or staff member/s of a service provider accesses The Company 's network to steal, copy, modify and/or delete sensitive personal information from inside the organisation. This type of breach can typically be achieved by ill-intentioned or aggrieved employees or service provider staff abusing their existing system credentials or installing malicious software onto The Company network.
Cloud service provider breach	Defined as a breach where a cloud service provider or The Company cloud-based platform is breached. Examples of such attacks are very similar in nature to an external breach except that the origin of the attack is typically at the cloud service provider, directly or indirectly affecting The Company.

Personal Identifiable Information (PII) breach	Defined as a breach achieved by any of the above means as well as procedural failures involving PII-related data. This type of breach must also be considered against the requirements defined in the POPI Act as it may require notification to the South African Information Regulator, and The Company Information Officer must be consulted in this regard.
Ransomware	Defined as a breach where a specialised form of malware is installed on The Company's network or an The Company owned device which completely encrypts computer systems into an unusable format. This form of encryption cannot be decrypted without a special key which only the attacker has in their possession and for which a ransom is demanded to decrypt the data. This is usually linked to a defined time period in which to pay the ransom
Device theft / loss	Defined as a security breach as a result of the loss or theft of data or equipment on which such data / personal information is stored (*e.g., loss of laptop, USB stick, iPad / tablet device, or paper record*)

1. OBJECTIVE AND PURPOSE OF THIS POLICY

1.1 The objective and purpose of this Policy is to outline a formal procedure to be followed by The Company and its Personnel in the event of a data breach which affects Personal Information held by The Company.

2. APPLICATION OF THIS POLICY

This Policy applies to all users of Personal Information within The Company environment, including employees, (permanent and temporary), The Company Directors, The Company Contractors and Service Providers, including Operators, as defined under POPIA, who will hereinafter be referred to as "Personnel".

3. INTERNAL REPORTING OF A DATA BREACH

3.1 If a Data Breach is suspected to have or is known to have occurred then Personnel must follow this below process:

3.1.1 immediately report to the Information Officer (or his/her Deputy Information Officer) any suspected or known data breach in writing, providing detail about the incident.

3.1.2 keep such information strictly private and confidential;

3.1.3 do not deal with any persons in relation to the data breach, this will be addressed by Information Officer and The Company Board Level;

3.1.4 Personnel must preserve all evidence relative to the Data Breach (actual or suspected);

3.1.5 Personnel must not do anything to the suspected computer/s or other system equipment which may be impacted or affected, including turning on or off, or shutting down the network, unless instructed to do so by The Investigatory Team; and

3.1.6 co-operate and fully support the Information Officer when asked about details of the incident.

4. INITIAL IDENTIFICATION, ASSESSMENT AND CONTAINMENT OF A DATA BREACH

4.1 In the event of a suspected or actual Data Breach an **Investigatory Team** will be assembled.

4.2 The Investigatory Team, should have appropriate:

4.2.1 internal representation - from the Information Officers and key departments such as IT, PR/Marketing and Legal, and should also have sufficient authority within The Company to investigate and address the incident in accordance with this Policy; and

4.2.2 external representation - to the extent that The Company does not have sufficient capacity internally to address the data breach in accordance with this Policy, The Company should appoint necessary external IT/forensic service providers and/or PR (in conjunction with their insurers (if applicable).

4.3 The Investigatory Team will ascertain if the incident involves a form of intrusion (via either internal or external threats) into The Company's physical and electronic systems which containment action could include:

4.3.1 identification of where the intrusion itself is occurring on the systems;

4.3.2 closing down such weak points to contain the incident; and

4.3.3 prevention of further impact on personal information through the compromised systems.

4.4 The Investigatory Team, is vested with the responsibility and duty to:

4.4.1 establish exactly what information has been compromised;

4.4.2 determine if the incident took place within the control of The Company;

4.4.3 evaluate the risk materialised within the control of its third parties. Process Guidelines for the establishment of the risk evaluation and incident classification appear at paragraph 5 of this Policy;

4.4.4 assess what obligations and responsibilities may flow under POPIA and also between The Company and third parties.

4.4.5 consider which other internal stakeholders should be informed of the incident and at what stage in the investigation process they should be informed (bearing in mind confidentiality and legal professional privilege considerations);

4.4.6 ensure that the investigation is kept confidential from those (internally or externally) that do not need to be made aware of the investigation (either wholly or in part) and

4.4.7 complete FORM 6 Data Breach Investigation Report;

4.4.8 notify The Company's broker and/or relevant insurer under any applicable cyber insurance Policy (or similar Policy).

4.4.9 in the event that an actual Data Breach is found to have occurred then, prepare a summary and provide recommendations to The Company Board, and also indicate whether there are **reasonable grounds** to believe that the Personal Information belonging to a person or legal entity (Data Subject) has been accessed or acquired by any unauthorised person. If such ground exist then the Investigatory Team **must** recommend to the Board that the matter be reported to i) Information Regulator; ii) the data Subject (if they can be identified); iii) any other law enforcement Agency as recommended iv) external expert legal representatives for advice on the notification requirements when in doubt.

4.4.10 Subject to paragraph 4.4.9 prepare the required communications to the Data Subject and Information Regulator.

5. PROCESS GUIDELINES FOR RISK EVALUATION AND INCIDENT CLASSIFICATION

5.1 All suspected and actual data breaches must be treated seriously.

5.2 The Investigatory Team should assess the risks arising from the data breach.

5.3 An assessment will require The Investigatory Team, to focus on determining factors such as the following (non-exhaustive):

5.3.1 what information was impacted by the data breach, categorise the risk (high/ medium low);

5.3.2 who is affected and identify the likelihood of any harm as a result of the incident;

5.3.3 where and by whom was the information being processed and handled and which The Company entity/ department / area / business / subsidiary / office is responsible for such processing and handling;

5.3.4 what was determined to be the root cause of the data breach;

5.3.5 what was determined to be the extent or reach of the data breach;

5.3.6 assess any potential adverse consequences to Data Subjects, clients / reputation; and/or Personnel of The Company.

5.4 Data Breach incidents should be classified according to severity of risk (High, Medium or Low Risk), considering the Risk Rating Table below and the following:

5.4.1 harm to Data Subjects whose personal information have been breached;

5.4.2 reputation damage, loss of profit / clients and the like to EIE Group; or

5.4.3 risk of legal action from Data Subjects or Information Regulator.

5.5 Other factors of the investigation will focus around whether or not the personal information involved in the incident was subject to specific protective measures. For example, i) was encryption used; ii) what levels of encryption were used; iii) was the encryption technology and the standard used sufficient to safeguard the Data Subjects against any risks as a result of the breach incident?

5.6 The formula for assessing data breach risks level of severity are as follows:

Severity	Definition
Level 1 $R \geq 4$	A security compromise in which the involved personal information may have a severe impact on Data Subjects and cause media, the public, or the Regulator's doubts on The Company's privacy protection and lead to severely negative consequences.
Level 2 $4 > R \geq 3$	A security compromise that leaks the Data Subjects' personal information and greatly affects the Data Subjects, while the risks can be reduced or even removed by taking some measures or means.
Level 3 $3 > R$	A security compromise in which personal information may be leaked while the leak has no impact or only a slight impact on the Data Subject.

5.7 All data breaches must be evaluated and classified in terms of the above table. This classification can be reviewed and adjusted appropriately accordingly as the Investigatory Team direct, in the course of their work.If the data breach and security compromise need to be notified, refer to the notification requirements set out below.

6. SECURITY COMPROMISE NOTIFICATION

Should The Company investigations, reasonably established that there has been unauthorized access or acquisition of personal information of any Data Subject i.e., a Data Breach then The Information Officer shall act in accordance with paragraph 4.3.9 and 4.3.10.

7. NOTIFICATION TO REGULATOR AND DATA SUBJECTS IN TERMS OF POPIA:

The Regulator must be notified of all unauthorised access or acquisition of personal information of any Data Subject, as soon as reasonably possible, which notification shall be in the form approved.

8. AFFECTED DATA SUBJECTS

8.1 All Data Subjects whose personal information was accessed or acquired in the data breach (unless their identity cannot be established), must be notified as soon as reasonably possible, or as directed by the Regulator, after the data breach incident in terms of POPIA.
8.2 Notification to the Data Subjects may only be delayed if the South African Police Service, the National Intelligence Agency or the Regulator determines that notification will harm a criminal investigation.
8.3 The notification to the affected Data Subjects must be in writing and communicated to the Data Subjects in at least one of the following ways, which manner of communication will be determined by the Board in conjunction with the Information Officer and where applicable, the Regulator: e-mail; placement on the website The Company; publication in the news media; or as may be directed by the Regulator.

9. REMEDIAL ACTION

In order to ensure that adequate remedial action is taken The Company must:
9.1 ensure that a risk register The Company is updated with all incidents and suspected incidents (near-misses);
9.2 update policies and procedures to ensure there will be measures to prevent future breach incidents of this type;
9.3 review any issues raised around service delivery / third party partners; and
9.4 finalise and implement the revised plan and conduct appropriate training.

10. DATA BREACH EVENT / INCIDENT EVALATION CLOSURE AND RECORD

10.1 The Company, must record the Data Breach for historical, trend, and legal purposes.
10.2 The Company must conduct an appropriate evaluation of each incident, to identity any particular weaknesses or failure points which lead to the incident arising.
10.3 The investigatory team should ensure that the lessons learned from the incident should be incorporated into strengthening the existing controls and procedures around data management and security.

11. CONSEQUENCES OF NON-COMPLIANCE

It is essential that all Personnel comply with all relevant parts of this Policy. Any failure to comply with this Policy could have serious consequences for The Company and its employees. Failure to comply may lead to disciplinary action, including summary dismissal for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

12. POLICY REVISION

This Policy has been reviewed and approved by the Information Officer and is subject to change without prior notice.

13. CONTACT DETAILS OF THE INFORMATION OFFICER

The details of the Information Officers of The Company are as follows:

West African International (Pty) Ltd (1995/008104/07)

WAG Chemicals (Pty)
(1986/003393/07)

6.1 Information Officer:-

Name	Brent Hean
Physical Address:	Lion Match Office Park, 892 Umgeni Road, Durban
Telephone Number	+27(31) 202 3900
Email	brent@westafricangroup.co.za
Information regulator Reference number	00654/2022-2023/IRRTT for West African International (Pty) Ltd 00629/2022-2023/IRRTT for WAG Chemicals (Pty) Ltd

a. Deputy Information Officers

Name	Cleopatra Ndlovu
Physical Address:	Lion Match Office Park, 892 Umgeni Road, Durban
Telephone Number	+27(31) 202 3900
Email	cleo@westafricangroup.co.za
Information regulator Reference number	00654/2022-2023/IRRTT for West African International (Pty) Ltd 00629/2022-2023/IRRTT for WAG Chemicals (Pty) Ltd

Name	**Grant Rosettenstein**
Physical Address:	Lion Match Office Park, 892 Umgeni Road, Durban
Telephone Number	+27(31) 202 3900
Email	grant@westafricangroup.co.za
Information regulator Reference number	00654/2022-2023/IRRTT for West African International (Pty) Ltd 00629/2022-2023/IRRTT for WAG Chemicals (Pty) Ltd

NAME	SIGNATURE	AUTHORISED FOR IMPLEMENTATION	VERSION