AECI Chem Park
2nd Floor, Block 2
200 Bergrivier Drive
Chloorkop Ext. 24
Kempton Park
South Africa, 1619
T +27 11 823 8000

Notification of security compromise in terms of Section 22(1)(b) of the Protection of Personal Information Act, 2013 – 13 February 2025

AECI Limited ("**AECI**") wishes to inform its stakeholders and potentially affected data subjects of an information security compromise on 4 January 2025. This notice provides information relating to the incident, the measures AECI has taken in order to mitigate any possible adverse effects, and recommendations on proactive steps which any potentially affected data subject may consider taking to secure their personal information.

AECI is taking measures reasonably necessary to determine the scope of the compromise and to restore the integrity of its information systems and servers. This is essential to ensure that personal information is not exposed to further risk. AECI has retained cybersecurity and forensic experts to work with its capable in-house IT team to manage this process.

Overview of incident

On Saturday, 4 January 2025 at around 08:06 am, AECI detected that a breach to one of its servers had taken place in its Nulandis.net portal. This portal is customer and agent facing, and serves AECI Plant Health, the AECI Agri Division of AECI.

Due to the encryption of the affected data by the threat actor, AECI remains unable to determine the exact number of affected data subjects. There is no evidence to suggest that the purpose or effect of the attack was to extract personal information for subsequent and malicious use. However, at this stage in the investigation, this possibility cannot be ruled out.

The review and forensic investigations is still underway to assess the unauthorised access to personal information and the number of categories of affected data subjects. However, the investigations at this stage indicate that the following categories of personal information may have been unlawfully accessed:

- Information relating to name, race, gender, sex, marital status, education
- Identify Numbers
- Tax information
- Financial statements & banking details
- Employment history
- Physical address
- Company registration details

AECI considers it prudent to assume that the abovementioned personal information may have been accessed and provides this notification to allow potentially affected data subjects and stakeholders to take protective measures against the possible consequences of the compromise.

What AECI has done

AECI takes the confidentiality, privacy and security of data and personal information in our care very seriously and were assisted by external forensic and legal specialists in responding to the incident. AECI has notified the Information Regulator (South Africa) of the incident.

AECI is in continuous efforts with its internal and external IT, forensic and legal specialists to understand the scope and impact of the incident and have implemented additional security measures by deploying enhanced endpoint detection and response software to detect unauthorised software on user devices. These are designed to enhance the existing security of its IT systems and to ensure the protection of data and personal information.

AECI is undertaking continuous monitoring for the publication of any data relating to AECI, or personal information of data subjects in its care, and its related entities on the internet and the dark web.

AECI will continue to evaluate additional measures to further strengthen its cybersecurity policies and procedures, and technological capabilities, to mitigate against the ever-evolving cyber risk landscape.

Possible consequences to data subjects

The affected categories of personal information may be used to attempt fraud or further security compromises to obtain additional personal information such as contact information to commit further unlawful activities. AECI recommends that all data subjects remain vigilant on any suspicious activities or fraudulent communication they may receive, specifically in relation to requests for banking information.

Although there is currently no evidence of any misuse of personal information potentially accessed, AECI encourages its stakeholders to safeguard their personal information by following these security measures, in accordance with best practice:

- Do not provide personal information in response to unsolicited emails, calls, or messages.
- Verify all requests for personal information and only disclose it when there is a legitimate reason to do so.
- Create complex passwords that are difficult to guess and use a different password for each account. Never share these with anyone else.
- Perform regular anti-virus and malware scans on your computer and mobile device, using software that is up to date.
- To mitigate any fraudulent consequences, you can place a fraud alert on your credit report at any of the major credit bureaus.

- You can register for a free Protective Registration listing with the Southern Africa Fraud Prevention Service (SAFPS) to help protect you against the risks of identity compromise (https://www.safps.org.za/Home/OurServices_ApplyProtectiveRegistration).

For more information

We remain committed to protecting the personal information which we process and prioritise the trust and privacy of our stakeholders.

If you have any questions or concerns or require more specific confirmation regarding the above, please write to us at planthealth@aeciworld.com.

AECI takes this matter extremely seriously and has dedicated the necessary resources to mitigating the impact of data subjects and other stakeholders.