cnr Ossewa Street & Norwalk Roads,
Chloorkop, Kempton Park, 1620
PO Box 150 Kempton Park 1620

T +27 (0) 11 921 3111
E info@ncp.co.za
www.ncp.co.za

2 August 2024

Dear Valued Stakeholder

Notification of security compromise

NCP Chlorchem (Pty) Ltd ("**NCP**" / **"we"**) hereby notifies you of an information security compromise that occurred on 15th January 2024 ("**the incident**"), in compliance with section 22 of the Protection of Personal Information Act, 2013 (POPIA).

Once the incident had been contained, we undertook a detailed review and analysis of the impacted data to understand the scope of the incident and to determine if personal information was affected. It has now been established that the personal information affected is confined to data subjects who underwent spirometer tests at NCP's facilities.

We are not aware of any leak of the impacted data or personal information as a result of the incident. We are providing information relating to the incident as well as the actions we have taken to date to mitigate any possible adverse effects of the incident. This is to ensure that any affected data subjects are aware of the incident and can take any additional measures they consider necessary to safeguard their personal information.

Overview of the incident

On 17th January 2024, we became aware that our IT environment was unlawfully accessed by an unidentified and unauthorised third party. A digital forensic investigation commenced immediately with the assistance of external subject matter specialists.

It was determined that the unauthorised third party managed to exfiltrate data and encrypt parts of our IT environment between 15th and 16th January 2024. There was limited impact on our business operations because we were able to restore most of the affected systems and servers from secure backups.

External IT specialists assisted NCP to analyse the impacted data to understand the nature, size and categories of personal information potentially impacted. It has been identified that the personal information affected was confined to spirometer (lung capacity) test results recorded by NCP between 2014 to 2017 for:

- employees who commenced their employment with NCP;
- employees who were re-tested over a two-year period;
- certain NCP plant personnel undergoing annual tests;
- employees undergoing exit medical tests; and
- external contractors who were tested in order to enter NCP's operations, who underwent annual spirometry assessments or were conducting business activities in NCP's facilities.

Company Registration No. 2003/017152/07 | VAT No. 4030219408

The following categories of personal information have been identified in the impacted data:

- Data Subject Name (Initials and Last Names)
- Age
- Date of Birth
- Phone Number(s)
- Organisation
- South African Identification Number
- Treating Doctor (Initials and Last Name)
- Specific disclosures relating to smoking status or chronic illnesses
- Gender
- Occupation and Department
- Height
- Weight
- Body Mass Index (BMI)
- Ethnicity
- Baseline Spirometry result (Flow Volume Test)

What we have done

We take the confidentiality, privacy and security of data and personal information in our care very seriously. We were assisted in responding to the incident by external forensic and legal specialists. The relevant regulators and law enforcement agencies have already been notified of the incident.

Robust security safeguards are already in place to protect data and personal information under our control. We have recovered fully from the incident and have implemented additional security measures which include:

- implementing password resets for all user accounts and securing NCP's file server by reapplying group server policies;
- strengthening remote access protocols, domain, and firewall password configuration;
- disabling and removing any legacy accounts and accounts not been used within 30 days; and
- deploying enhanced endpoint detection and response (EDR) software to detect unauthorised software on user devices.

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.

We encourage you, in accordance with best practice, to maintain these security safeguards:

- 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.

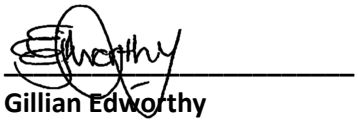
- Create complex passwords that are difficult to guess and use a different password for each account. Never share these with anyone else.
- Perform regular anti-virus and malware scans on your computer and mobile device, using software that is up to date.

For more information

We remain committed to protecting the personal information which we process.

If you have any questions or concerns or require more specific confirmation as to whether any of your personal information appears in the impacted data, please write to us at *informationofficer@ncp.co.za.*

Yours sincerely,



Gillian Edworthy
GRC Director