

## ARMCO SUPERLITE (PTY) LTD

131 Anvil Road, Isando, Gauteng, 1600

**Tel:** +27 (0)11 974 8511 | **Email:** Fourie.sean@armco.co.za

**Website:** www.armco.co.za

**Date:** 22 October 2026

**To:** Valued Customers and Business Partners

**Subject:** Important Security Notice: Unauthorized Email Account Incident

Dear Valued Customer,

At **Armco Superlite (Pty) Ltd**, the privacy, security, and integrity of your information and business communications are of paramount importance to us. In line with our commitment to transparency and responsible governance, we are writing to inform you of a recent cybersecurity incident involving unauthorized access to a limited number of our business email accounts.

### What Happened?

On **21 October 2026**, our IT and cybersecurity team detected anomalous activity originating from specific email accounts within our Microsoft 365 environment. We immediately launched a containment and digital forensic investigation.

The investigation determined that unauthorized access to these mailboxes commenced on or about **30 September 2026**. As a result, certain email correspondence and attachments exchanged between our team and external contacts during this window may have been viewed or accessed by an unauthorized third party.

### What Information Was Involved?

The incident was strictly confined to specific email accounts and their associated message threads. This correspondence may have included:

- Contact details (e.g., employee/client names, business email addresses, and phone numbers).
- Commercial correspondence, requests for quotations, order acknowledgments, and purchase orders.
- Historical delivery notes, invoices, or general billing inquiries.

*Please note: Our core databases, SYSPRO Enterprise Resource Planning (ERP) systems, financial platforms, and operational production networks remain fully secure and were **not** compromised or impacted.*

### Actions Taken and Preventative Measures

Immediately upon discovery on 21 October 2026, our IT team initiated robust containment and remediation measures:

1. **Immediate Containment & Revocation:** All active user sessions associated with affected accounts were terminated immediately, and global credential resets were enforced.
2. **Access Control & Multi-Factor Authentication (MFA):** We verified and enforced phishing-resistant Multi-Factor Authentication (MFA) across all organizational email and cloud applications.

3. **Mailbox Rules & Delegate Audit:** We conducted a comprehensive audit of all email inbox forwarding rules, connector permissions, transport configurations, and API delegates to ensure no persistence mechanisms or backdoors remained.
4. **Enhanced Endpoint & Identity Monitoring:** We deployed tightened conditional access policies, geo-blocking controls, and automated threat alerts to detect and block abnormal sign-in behaviours in real time.
5. **Regulatory Compliance:** In accordance with Section 22 of the Protection of Personal Information Act (POPIA), we are taking the necessary steps to notify the Information Regulator of South Africa.

### Recommended Precautionary Steps

While the incident is fully contained, threat actors frequently attempt to leverage historical email correspondence for targeted phishing or payment diversion fraud. We advise our partners and customers to exercise the following precautions:

- **Verify Banking & Payment Requests:** Armco Superlite will **never** notify customers of changes to banking or remittance details via an unverified email. If you receive any notification or invoice requesting payment to an altered bank account, **do not proceed**. Immediately verify the authenticity telephonically using known, verified branch contact numbers before processing any transaction.
- **Remain Vigilant:** Treat unexpected requests for passwords, urgent funds transfers, or emails containing unusual links or unsolicited attachments with caution.
- **Report Suspicious Correspondence:** If you receive an email purporting to be from Armco Superlite that appears suspicious, irregular, or out of context, please notify us immediately.

### We Are Here to Support You

We sincerely regret any concern or inconvenience this incident may cause. We take our responsibility to safeguard our customer and partner communications seriously and continue to reinforce our defenses against emerging cyber threats.

If you have questions, require verification of recent correspondence, or would like to discuss this notice with our technical team, please contact us directly:

- **Dedicated Contact POPIA: Tamarin Temblett**
- **Email:** temblett.tamarin@armco.co.za
- **Direct Office Line:** +27 (0)11 974 8511

Sincerely,

Armco Superlite (PTY) Ltd