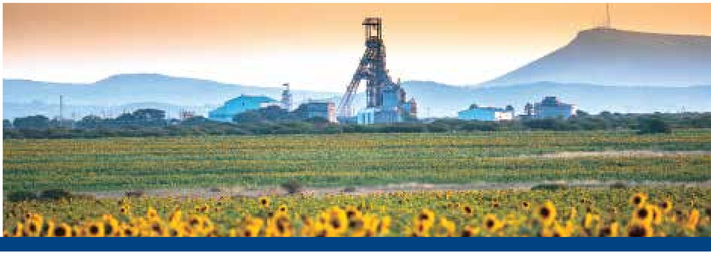

INFORMATION AND CYBERSECURITY POLICY STATEMENT

At Implats, we understand that information is one of our most critical assets. We are dedicated to ensuring the confidentiality, integrity and availability of all information under our stewardship. Protecting data is a strategic business priority and a reflection of our commitment to our clients, subsidiaries and stakeholders. Our Information and Cybersecurity Policy serves as the cornerstone of our efforts to manage information and cyber risks across our operations, encompassing both information technology (IT) and operational technology (OT) environments.

Implats' policy includes our objectives and commitment to:

- **Protect information assets:** Ensure all company and stakeholder data is safeguarded against unauthorised access, disclosure, alteration or destruction by enforcing robust access controls and multi-factor authentication
- **Ensure business continuity:** Maintain the resilience of systems and processes to minimise operational disruptions and support uninterrupted business operations
- **Maintain legal and regulatory compliance:** Adhere to all relevant laws, industry standards and contractual obligations related to information and cybersecurity
- **Foster a security-conscious culture:** Promote awareness and accountability among employees through ongoing training and consistent communication across established platforms
- **Apply risk-based security controls:** Implement appropriate technical and organisational measures based on thorough risk assessments to address potential threats and vulnerabilities
- **Monitor and improve continuously:** Leverage advanced monitoring tools and conduct regular reviews to enhance our information and cybersecurity practices in response to evolving threats and technologies
- **Respond effectively to security incidents:** Act swiftly and transparently using approved incident response plans and conduct regular cyber-incident simulations to ensure preparedness.

Information Security Management Programme (ISMP)

Implats' Information Security Management System is structured in alignment with globally recognised standards, including ISO/IEC 27001, NIST and CIS Critical Security Controls (CIS CSC). It undergoes continuous review and enhancement to stay ahead of emerging threats and evolving technologies.

Key elements of our ISMP Include:

- **Policy foundations:** All principles and elements outlined in our Information and Cybersecurity Policy form the core of our security management practices
- **Governance and leadership:** The ISMP is overseen by the Implats board's audit and risk committee, with strategic direction and oversight provided by executive leadership to ensure alignment with business goals and regulatory obligations
- **Risk-based approach:** We perform regular risk assessments to proactively identify, evaluate and mitigate information security risks across both our IT and OT environments
- **Policies and procedures:** A comprehensive framework of security policies, standards and procedures guides employees, contractors and partners in upholding secure and compliant practices
- **Vulnerability management:** We conduct routine vulnerability scans and assessments to detect and address potential weaknesses in our systems and infrastructure
- **Third-party risk management:** We evaluate and monitor the cybersecurity posture of our suppliers, contractors and technology partners through structured third-party risk assessments to ensure holistic protection
- **Incident reporting, response and recovery:** Our established incident response procedures enable rapid detection, containment and recovery from security incidents, minimising operational disruption and supporting business continuity.

(All policies and procedures and plans are provided as evidence to substantiate the statements above)

Asad Rajab – *Chief Information Officer* • September 2025

RESPECT, CARE
AND DELIVER

IMPLATS
EXCELLENCE IN PGMs