

# INFORMATION SECURITY POLICY



As one of the world's leading recycling organisations, we are committed to implementing an effective Information Security Management System (ISMS) in order to achieve our intended outcomes which are to ensure the protection of our business information assets which includes employee, customer and supplier data. Reputation is a key business asset and the ISMS will ensure that EMR Group's reputation for the management of information is protected.

EMR Group's Senior Leadership will demonstrate commitment to effective information security management and will ensure that all personnel are aware of the Company's information security aims and objectives through the delivery of ongoing training and internal communications.

EMR Group aims to achieve specific, defined information security objectives, which are developed for all EMR Group companies and subsidiaries in accordance with the business objectives, the context of the organisation, the results of risk assessments, and the risk treatment plan. All employees of EMR Group are expected to comply with this policy and with the ISMS that implements this policy. The consequences of breaching the information security policy are set out in the Company's disciplinary policy and in contracts and agreements with third parties.

## Objectives

- All management, full or part time employees, agency workers, contractors, project consultants, and any external parties have, and will be made aware of, their responsibilities to preserve information security, to report security breaches, and to act in accordance with the requirements of the ISMS.
- Ensure information assets are accessible to authorised users when required. To prevent unauthorised access to all personal information of employees and customers and to have zero reportable data breaches.
- To reduce the overall Information Security risk score by 25%.
- Ensure that employees and agency workers receive training and awareness specific to Information Security within EMR.
- Provide a simple method for the reporting and management of all Information Security Incidents.
- Create an Information Security aware culture where Information Security is discussed and considered at all levels.
- Hold regular reviews of our policy, systems and practices to ensure continual improvement in our Information Security Management System.

EMR Group provides access to many different information systems and their use carries with it, the responsibility to use these systems in a safe and secure manner. Effective security is a team effort involving the participation and support of every EMR Group employee and affiliate who deals with information and/or information systems. It is the responsibility of everyone to read, understand, and follow these guidelines, and to conduct their activities accordingly.

This policy will be displayed in every depot, communicated to everyone working for or on behalf of EMR and displayed on our website.

This statement is signed by the Group Chief Information Officer on behalf of the Board and the Executive Management Team to demonstrate the commitment of the Company and operationally to this goal.



Joe Macken  
**Group CIO**

September 2019



Edwin Leijnse  
**Group COO**

September 2019