CYBER SECURITY POLICY

This cyber security policy outlines the compulsory requirements that all Insert Your Company personnel, agencies and associates must follow, to ensure that cyber security risks to information and data systems are appropriately managed and kept secure.

This cyber security policy applies to all:

- Information, data, software and digital assets created and managed by Insert Your Company including any out-sourced information, data and digital assets.
- Information and communications of technology systems.
- Operational technology and 'internet of things' devices that manage data or provide any Insert Your Company digital service.

Exemptions to this cyber security policy will only be considered in exceptional circumstances. If an exemption request is deemed to be valid by Insert Your Company management, a documented response will be provided and must be strictly followed.

[illegible]

[illegible] are kept secure by:

- [illegible]
- [illegible]
- Not leaving their devices unattended or exposed.
- Ensuring that their devices have modern and up to date antivirus software.
- Updating the security software and systems as soon as the updates are available.

Email Security

All personnel must report suspicious emails and avoid opening such emails unless they are certain the source is trustworthy.

Personnel are further instructed to:

- Be suspicious of clickbait titles with enticing information or rewards.
- Avoid opening attachments or links where the content is suspicious or invitingly vague.
- Always block junk, spam and scam emails.
- Be wary of inconsistent and poorly formatted emails that appear to come from unprofessional sources.
- Always verify unfamiliar or unknown email sources before opening.

Password and Credential Management

Passwords and associated credentials must always be kept secure. Accordingly, password holders must:

- Not leave devices unattended without enabling a password-protected screensaver or logging off the device.
- Protect their passwords and credentials by ensuring that the internet browsers used on shared or public devices do not store their username or password.
- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid passwords that can be easily predicted.