Please amend any text or sections as you feel appropriate.
All red lettering needs to be amended and deleted.
For a more personalised appearance, please print on your company letterhead or add your company logo.

Cyber Security Policy inc.

Cyber Security Incident Response

PURPOSE OF THIS POLICY:

The purpose of this Cyber Security Policy is to protect **[INSERT COMPANY NAME]** information assets from all threats, be those threats external or internal, or malicious or accidental. This will ensure business safety continuity, and will minimise business disturbance, damage or destruction. This in turn will provide maximum return on all developments, investments and opportunities.

OBJECTIVE OF THIS POLICY:

The objective of this Cyber Security Policy is for **[INSERT COMPANY NAME]** to be prepared to respond to any cyber security incidents, and prevent disruption to the business by providing required controls for incident handling, reporting and monitoring, and incident response and assistance.

RESPONSIBILTIES:

All users of **[INSERT COMPANY NAME]** computing resources shall be aware of what constitutes a cyber security incident and shall understand all incident reporting procedures and monitoring.

POLICY:

- The **[MANAGING DIRECTOR]** of **[INSERT COMPANY NAME]** has indeed approved this all information contained within this Cyber Security Policy

- It is the Policy of **[INSERT COMPANY NAME]** to constantly ensure that:

    - All breaches of information security (true or suspected) will be reported in the first instance to, and investigated by, the named Information Security Manager.
    - All information will be protected from a loss of confidentiality (App 2), sincerity (App 3) and connection (App 4).
    - All aspects of regulatory and legislative requirements will be met (App 5).
    - Business continuity plans will be produced, maintained and tested (App 6).
    - Information security training will be provided to all **[INSERT COMPANY NAME]** employees.
    - Metrics required for measuring the incident response will be provided by **[INSERT COMPANY NAME]**

GUIDANCE AND PROCEDURES:

- Guidance and procedures will be produced to support this policy in full. These may/will include (but are not limited to) data protection, credit card handling, information classification, incident handling, information backup, malware controls, mobile device security, remote working measures, risk assessment, system access, third party services (supplier due diligence), passwords and encryption.

  - The roles and responsibilities of the named Information Security Manager (App 7) are to manage information security, provide up to date advice and guidance on implementation of the Information Security Policy, provide up to date technology to maintain the security of the information security. **[The policy needs supporting documents and work instructions which covering every aspect of the policy]**

- The named owner of the Information Security Policy has full responsibility for maintaining and reviewing the Information Security Policy.

- All managers of **[INSERT COMPANY NAME]** are fully responsible for implementing the Information Security Policy within their business remit.

- It is the responsibility of each individual employee to adhere fully to the Information Security Policy.

Print _____

Signed _____

Title _____

Date _____

APP.

1. Information can take on a variety of forms. The definition of information within this policy includes data printed or written, electronically stored data, data conducted by postal service or electronic means, stored data in any form, data released on an oral basis.
2. Confidentiality. To constantly maintain, monitor and ensure that all information and data is only accessible to authorised personnel.
3. Sincerity. To safeguard the accuracy, timeliness and completeness of information and processing methods.
4. Connection. To ensure that only authorised users have access to relevant information, as and when required.
5. Including the requirements including, but not limited to, Companies Act 2006, Computer Misuse Act 2011, the Copyright, Design and Patents Act 1988, and the Data Protection Act 2018.
6. Contingencies to ensure that information and vital services are always available to authorised personnel.
7. Depending on the type and size of the business this may be a part or full-time role for the nominated person.