WEST COAST RISK LIMITED

SECURITY POLICY

WCR-SEC-POL-0001

POLICY STATEMENT

At West Coast Risk, we are committed to maintaining a robust physical security operation that ensures the safety and protection of our client's staff and assets, whilst maintaining respect for human rights. We understand the importance of implementing effective access control measures, surveillance systems, and asset protection protocols to safeguard our facilities and maintain operational integrity.

Through continuous improvement and regular audits, we will strive to stay ahead of potential security risks and ensure compliance with industry best practices.

Our commitment to physical security aligns with our core values of **safety, integrity**, and **respect for human rights**. Together, we will create a safe and secure working environment that enables us to achieve our goals and objectives.

"Security is everybody's responsibility and by following this security policy, we aim to create a safe and secure environment for all individuals associated with West Coast Risk Corporation Ltd."

David Butler

Managing Director

West Coast Risk Corporation Ltd

Table of Contents

1. INTRODUCTION

West Coast Risk Corporation Limited (WCR) is committed to maintaining the highest level of security for its employees, contractors, visitors, and assets across all its sites. This security policy outlines the principles, guidelines, and procedures that govern security practices within the organisation, aligning with the company's core values.

2. SCOPE

The policy applies to all employees, contractors, visitors, and third-party individuals who access West Coast Risk’s facilities, data, and resources. It encompasses all physical, technical, and administrative security measures.

3. OBJECTIVE

The primary objective of this security policy is to ensure the protection of West Coast Risk's people, information, physical assets, and reputation. By implementing and adhering to this policy, West Coast Risk aims to create a secure environment that promotes the safety and well-being of all stakeholders.

4. PHYSICAL SECURITY

4.1 Access Control:

Access control measures exist at all its sites to restrict unauthorised entry to its facilities. Access control measures and visitor management protocols are carried out by security provider and are utilised to monitor regular access.

4.2 Asset Protection

Control measures exist to protect physical assets, including equipment, machinery, and valuable resources. Security measures such as secure storage, alarm systems and inventory controls are implemented across all sites to safeguard assets from theft, damage, or unauthorized use. Regular asset audits and inspections are to be conducted to ensure compliance.

4.3 Surveillance:

Security cameras and monitoring systems are installed at strategic locations to enhance surveillance and deter potential security threats.

4.4 Emergency Response:

West Coast Risk has well established emergency response procedures, including evacuation plans, fire drills, and incident reporting processes to ensure a prompt and efficient response to emergencies.

4.5 Proportional Response:

Security forces used at West Coast Risk are non-armed officers. However, if no other alternative exists to properly manage the threat, police support may be used in the scope of international codes of conduct, such as the Voluntary Principles for security and Human Rights, legal and government approved practices.

5. INFORMATION SECURITY

5.1 Data Protection:

West Coast Risk ensures appropriate measures are in place to protect sensitive information from unauthorised access, disclosure, alteration, or destruction. This includes but is not limited to the use of passwords, encryption, and data backup.

5.2 Information Security Awareness:

Regular training and awareness programmes are conducted to educate employees and contractors about information security best practices, including the identification and handling of sensitive data.

5.3 Incident Response:

West Coast Risk has established effective incident response procedures to promptly address and mitigate security incidents, including data breaches, malware attacks, and unauthorised access.

6. NETWORK SECURITY

6.1 Firewall and Intrusion Detection:

West Coast Risk employs firewalls and intrusion detection systems at all its sites to monitor and protect its network infrastructure from unauthorised access and malicious activities.

6.2 User Access Control:

Access to computer systems and networks across all sites should be granted based on role-based access control (RBAC) principles. User accounts are regularly audited and deactivated upon termination or transfer.

7. BUSINESS CONTINUITY

7.1 Business Continuity Analysis:

West Coast Risk conducts periodic analysis of business continuity plans to identify critical business functions and determine their recovery priorities in the event of disruption.

7.2 Crisis Management Plan:

A comprehensive Crisis Management Plan is being developed to ensure the timely restoration of critical systems and data in the event of a disaster or major disruption.

7.3 Regular Backups:

West Coast Risk implements regular backup procedures at all sites to safeguard critical data and facilitate recovery in the event of data loss or system failure.

8. COMPLIANCE

West Coast Risk is committed to complying with all applicable laws, regulations, and industry standards related to security across all its sites.

9. REPORTING AND MONITORING

West Coast Risk has well established mechanisms to monitor and assess the effectiveness of security controls across all sites. Incidents and security breaches are reported promptly to the appropriate authorities for investigation and resolution.

10. SYSTEM EVALUATION

This policy shall be reviewed at least after two years by members of the Security Department and presented to the Standard Committee for approval, or when organizational changes take place or required as part of internal and external audits. The WCR Document Controller will monitor compliance with the document control system on an ongoing basis.

11. DISTRIBUTION

List physical locations which require a controlled copy of this document.

Copy	Controlled Document Folder Location
Master	Controlled Documents Central Filing System

13. CONTRAVENTION

Any breach of this policy shall be regarded as refusal/failure to carry out a lawful instruction and will be dealt with as per the disciplinary procedure.

14. DOCUMENT CHANGE PROCESS

The process of document change starts when the document custodian identifies there is need to make changes within the document. The document custodian/ owner shall complete the document change request form, sign it off and submit it to the Document Controller.

The Document controller shall issue the controlled word copy of the document to the respective document custodian/owner so that changes may be made. The document custodian/owner shall resubmit the updated document to the document controller so that the document can be controlled and updated within the Filing system ready for use by the end users.