# Castor Vali
# Security Management Policy

## Table of Contents

1 Policy Statement ..... 3
1.1 Purpose ..... 3
1.2 Scope ..... 3
1.3 Compliance with Local Legislation ..... 4
1.4 Definitions ..... 4
2 Roles and Responsibilities ..... 4
3 Procedures and Guidelines ..... 5
3.1 Leadership and Governance ..... 5
3.2 Security Objectives and Performance ..... 5
3.3 Risk and Human Rights Management ..... 6
3.4 Client Acceptance and Operational Control ..... 6
3.5 Use of Force and Armed Support ..... 6
3.6 Personnel and Competence ..... 7
3.7 Suppliers, Subcontractors and Operational Partners ..... 7
3.8 Security Resources and Asset Protection ..... 7
3.9 Communication, Consultation and Awareness ..... 7
3.10 Incident, Crisis and Continuity Management ..... 8
3.11 Complaints, Whistleblowing and Remedy ..... 8
3.12 Documented Information ..... 8
4 Monitoring and Enforcement ..... 8
5 Policy Review and Updates ..... 9

# 1 Policy Statement

Castor Vali is committed to providing and managing professional, lawful, ethical and accountable security and risk-management services that protect clients, personnel, assets and affected communities while respecting human rights.

The company will establish, implement, maintain and continually improve its Security Operations Management System as an integral part of the Integrated Management System. Security operations will be planned and delivered using intelligence-led, risk-based and proportionate controls appropriate to the legal, human-rights, contractual and operational context.

Castor Vali will comply with applicable legal, regulatory, licensing and contractual requirements and with the voluntary commitments to which it subscribes, including the International Code of Conduct for Private Security Service Providers, the Montreux Document, the United Nations Guiding Principles on Business and Human Rights and the Voluntary Principles on Security and Human Rights.

The company is committed to avoiding, preventing and reducing the likelihood and consequences of disruptive or undesirable events; providing effective remedy where Castor Vali has caused or contributed to an adverse impact; and continually improving the suitability, adequacy and effectiveness of its security-management arrangements.

## 1.1 Purpose

The purpose of this Policy is to:

- provide the governing policy framework for Castor Vali's security operations and management arrangements for ISO 18788 and ISO 28007;
- establish the principles against which security objectives, operational controls and performance measures are set and reviewed;
- integrate lawful conduct, human rights, risk management and stakeholder requirements into business and operational decision-making;
- define leadership accountability and the responsibilities of personnel working for or on behalf of Castor Vali;
- ensure that services, suppliers, subcontractors and operational partners are managed in a manner proportionate to their risks; and
- support monitoring, assurance, learning and continual improvement across the Group.

## 1.2 Scope

This Policy applies throughout the Castor Vali Group and to all entities governed by the shared Integrated Management System. It applies to directors, employees, individual contractors, embedded personnel and, where relevant to the services they provide, suppliers, subcontractors, local partners and other parties working for or on behalf of Castor Vali.

It covers the provision and management of armed and unarmed security, intelligence-led risk management and advisory services within land and maritime environments, including:

- unarmed guarding and protective services;
- embedded security and risk-management personnel;
- mobile security, close protection and journey management;
- risk intelligence, monitoring, analysis and advisory services;
- offshore and maritime security services;
- subcontracted Private Contracted Armed Security Personnel services for vessels operating within the high-risk areas of the Gulf of Aden, East Coast of Africa and Indian Ocean; and
- exceptional support provided by host-nation police, military, navy or other duly authorised state security forces.

The Policy also applies to the corporate, information, physical, personnel, financial and supply-chain arrangements that support security operations.

### 1.3 Compliance with Local Legislation

This Policy provides a standardised approach to security management across Castor Vali. It shall be interpreted and applied together with applicable international, national and local law, licensing conditions, regulatory requirements, contractual obligations and recognised human-rights commitments in the relevant country and area of operation.

Where legal or contractual requirements differ between jurisdictions, Castor Vali shall apply the requirement that is legally binding and provides appropriate protection. Any conflict, ambiguity or concern that an instruction could result in unlawful conduct or an adverse human-rights impact shall be escalated before the activity proceeds. No client instruction, commercial objective or local practice justifies unlawful conduct or a breach of Castor Vali's human-rights commitments.

### 1.4 Definitions

**Security Operations Management System:** The part of Castor Vali's Integrated Management System used to direct, control and continually improve the management of security operations in accordance with ISO 18788 and ISO 28007.

**Security operation:** An activity undertaken to protect people, assets, information, locations, vessels or operations, or to provide security-related risk management, intelligence or advice.

**Host-nation security forces:** Police, military, navy or other state security personnel who provide protection or support within their own legal authority and chain of command.

**PCASP:** Privately Contracted Armed Security Personnel deployed on board ships in accordance with applicable law, flag-state requirements, contractual arrangements and recognised maritime-security standards.

**Affected stakeholders:** Individuals, groups or organisations that may affect, be affected by or perceive themselves to be affected by Castor Vali's activities, including workers, clients, protected persons, authorities, suppliers, subcontractors and local communities.

## 2 Roles and Responsibilities

| Role | Responsibilities |
|---|---|
| **CEO and C-Suite** | Provide top-management leadership; approve and visibly endorse this Policy and the Statement of Conformance; ensure integration with business strategy; provide adequate resources; review performance; and promote continual improvement. |
| **Chief Operating Officer** | Own the Security Operations Management System; oversee implementation and day-to-day performance; ensure management-system requirements are integrated and communicated; report performance to top management; and coordinate Management Review and improvement action. |
| **Compliance Manager** | Support conformity with ISO 18788 and applicable legal, regulatory and voluntary commitments; maintain compliance information; coordinate assurance activity; and advise management on nonconformities and required action. |
| **Service Area Champions** | Ensure the requirements of this Policy are applied within Corporate Risk Services, Offshore and Maritime Services and Risk Intelligence Services, including the definition of service-specific controls, competence and performance requirements. |
| **Head of Operations** | Oversee physical security operations; ensure appropriate operational planning, resources, risk controls, communications, supervision, incident response and performance monitoring; and escalate unacceptable risks. |
| **Country Managers** | Ensure legal, licensing, client and IMS requirements are implemented within their jurisdictions; provide appropriate resources and oversight; and report significant risks, incidents, complaints and performance matters. |

| | |
|---|---|
| **Project and Operations Managers** | Confirm that tasks are lawful, risk assessed, adequately resourced and approved; brief personnel and operational partners; monitor delivery; maintain required records; and suspend, modify or decline activities where risks cannot be controlled. |
| **Head of Risk Intelligence Services** | Ensure intelligence products and alerts are timely, relevant, reliable and appropriately communicated to support strategic and operational decision-making. |
| **Human Resources and Training** | Support recruitment, vetting, competence, induction, training, awareness, welfare and performance-management requirements for personnel engaged in security operations. |
| **Procurement and Contract Owners** | Apply risk-based due diligence, approval, contracting and monitoring controls to suppliers, subcontractors and operational partners. |
| **All Personnel** | Comply with this Policy and applicable instructions; contribute to effective security operations; report risks, incidents, concerns and potential nonconformities; and exercise stop-work authority where an activity may be unsafe, unlawful, unethical or inconsistent with human-rights commitments. |

# 3 Procedures and Guidelines

## 3.1 Leadership and Governance

Top management shall demonstrate active leadership by integrating security-management requirements into business processes, providing adequate personnel and resources, supporting responsible managers, communicating the importance of lawful and effective security operations and reviewing performance at planned intervals.

The CEO retains executive ownership of the Integrated Management System. The COO is responsible for its day-to-day management and performance reporting, supported by the Compliance Manager, service-area champions, functional heads and country management. Responsibilities and authorities shall be defined in organisational charts, role descriptions and relevant controlled documents.

Castor Vali's Statement of Conformance and Applicability sets out the organisation's commitment to respect human rights and its application of ISO 18788. It shall be maintained, visibly endorsed by top management and made available to relevant internal and external stakeholders.

## 3.2 Security Objectives and Performance

Security objectives shall be established at relevant functions and levels and shall be consistent with this Policy, the company's strategic direction and the risks and opportunities affecting security operations. Objectives shall, where practicable, be measurable and shall identify responsibility, resources, target dates, monitoring arrangements and the intended result.

The objective framework shall include, as applicable:

- lawful, professional and human-rights-respecting service delivery;
- effective identification and treatment of security, safety and human-rights risks;
- prevention and reduction of disruptive or undesirable events;
- competent, vetted and appropriately briefed personnel;
- effective oversight of suppliers, subcontractors, PCASP providers and host-nation security forces;
- timely reporting, investigation and resolution of incidents, complaints and nonconformities;
- effective crisis preparedness, communications and operational resilience;
- client and stakeholder confidence; and
- continual improvement of security operations and the management system.

Progress shall be monitored using suitable performance information and reviewed through operational management, internal audit, compliance evaluation and Management Review. Where objectives are not achieved, the cause and required corrective or improvement action shall be determined.

### 3.3 Risk and Human Rights Management

Castor Vali shall identify, assess, treat and monitor risks and opportunities affecting the organisation, its security operations and relevant supply-chain relationships. Assessment shall consider applicable law, licensing, contractual obligations, the threat and operating environment, human rights, safety, environmental conditions, communities, reputation, resources, competence and the potential consequences of failure.

Human-rights risk and impact assessment shall be proportionate to the location, service, client, stakeholder relationships and operational risk. Elevated risks shall be subject to enhanced review, approval, treatment, monitoring and, where required, a project-specific Human Rights Impact Assessment.

Security operations shall not proceed where the legal authority is unclear, required resources or controls are unavailable, or residual risk exceeds approved parameters. Personnel may pause or stop an activity where there is an immediate threat to safety, security, human rights or legal compliance. Significant residual risk shall be escalated to the COO or another appropriate Group Director.

### 3.4 Client Acceptance and Operational Control

Client requirements shall be reviewed before acceptance to confirm that the service is lawful, ethical, within Castor Vali's competence and capability and capable of being delivered with appropriate resources and controls. Security, legal, contractual and human-rights requirements shall be incorporated into contracts, operational plans, risk assessments, task instructions, post orders, briefings or other controlled documentation as appropriate.

Operational acceptance criteria, authority levels and approvals shall be proportionate to the scale, complexity and risk of the task. Planned and dynamic changes shall be assessed, authorised and communicated. Castor Vali may modify, suspend or decline a service where the client does not accept controls necessary to reduce risk to an acceptable level.

Personnel shall be briefed on their duties, authority, limitations, risk controls, communications, incident reporting and escalation arrangements before deployment. Supervisors shall monitor delivery and correct deviations from approved requirements.

### 3.5 Use of Force and Armed Support

Castor Vali seeks to avoid the use of force through prevention, communication, de-escalation, withdrawal and other reasonable alternatives. Any use of force must be lawful, necessary, proportionate to the threat and limited to the minimum reasonable force required. Incidents involving actual or alleged use of force shall be reported, investigated and reviewed in accordance with company requirements and applicable law.

Castor Vali does not own, store, transport, issue or account for firearms, ammunition or less-lethal weapons. Armed support is provided only through appropriately authorised host-nation security forces or subcontracted PCASP providers. Such parties remain responsible for their weapons, legal authority, rules of engagement or use of force and chain of command.

Where armed support is used, Castor Vali shall define its requirements through due diligence, contracting, liaison, task planning and briefings. These arrangements shall address lawful authority, command boundaries, communications, escalation, human-rights expectations, use-of-force expectations, incident reporting and Castor Vali's right to suspend or withdraw from an operation where conduct is unlawful or inconsistent with agreed requirements.

### 3.6 Personnel and Competence

Personnel performing work that may affect security operations shall be selected, vetted, competent and fit for their assigned responsibilities. Competence requirements shall be defined through role descriptions, legal and licensing requirements, client requirements, risk assessments and the Group competence framework.

Employees, contractors, embedded personnel and relevant subcontractor personnel shall receive induction, task-specific instruction and refresher training proportionate to their role and risks. Training shall include applicable conduct, human-rights, reporting, safety, security and operational requirements. Competence and training records shall be retained, and identified gaps shall result in training, supervision, reassignment or removal from the task as appropriate.

### 3.7 Suppliers, Subcontractors and Operational Partners

Suppliers, subcontractors, PCASP providers and other operational partners shall be subject to risk-based due diligence, approval, contracting, tasking and performance monitoring proportionate to their potential impact on security operations. Relevant controls shall address competence, licensing, legal and human-rights performance, conduct, insurance, financial and operational capacity, incident reporting, information security and service reliability.

Castor Vali retains accountability for the outsourced processes and services it manages. Deviations, waivers and conditional approvals shall be authorised, limited, recorded and monitored, with outstanding due diligence completed as soon as practicable.

Host-nation security forces are not Castor Vali suppliers and remain outside the company's command. Nevertheless, where they support a Castor Vali-managed operation, their lawful authority, role, command boundaries, communications, escalation, human-rights and use-of-force expectations shall be considered and documented proportionately within operational planning.

### 3.8 Security Resources and Asset Protection

Before accepting or commencing an operation, Castor Vali shall determine and provide the competent personnel, intelligence, equipment, vehicles, communications, medical support, logistics, technology, finance and external services necessary to deliver it safely and effectively. Required resources shall be derived from risk assessments, client requirements, operational plans and applicable procedures.

Operational equipment, vehicles and communications shall be inspected or tested before deployment as applicable. Where essential resources are unavailable, defective or become inadequate, the activity shall be delayed, modified, suspended or otherwise controlled until acceptable arrangements are restored.

Physical and information assets shall be protected against unauthorised access, loss, damage, disclosure, alteration or disruption through access control, secure handling, cybersecurity, business-continuity and incident-management arrangements proportionate to the risk.

### 3.9 Communication, Consultation and Awareness

Castor Vali shall determine what security-related information must be communicated, when, to whom, by whom and through which method. Communication arrangements shall include personnel, clients, protected persons, suppliers, subcontractors, authorities, host-nation security forces and affected communities where relevant.

Significant risks, controls, changes, alerts, incidents and escalation requirements shall be communicated promptly through approved operational channels. Communications capability shall be maintained and tested under normal and disruptive conditions, with suitable primary and backup arrangements.

This Policy and the Statement of Conformance shall be communicated to relevant employees, contractors and other persons working for or on behalf of Castor Vali through induction, refresher training, SharePoint, contracts, task briefings and other appropriate channels. Key policies shall be made available to external stakeholders through the company website or on request.

### 3.10 Incident, Crisis and Continuity Management

Castor Vali shall maintain arrangements to identify, report, assess, respond to, investigate and learn from security incidents, emergencies and disruptive events. Response arrangements shall be scalable and shall define authority, escalation, command, communications, stakeholder notification, evidence preservation, welfare and recovery requirements.

Significant incidents, including alleged human-rights violations, use-of-force events, serious misconduct and material failures involving suppliers, subcontractors or host-nation security forces, shall receive prompt management attention and appropriate notification. Root causes, lessons, corrective action and effectiveness evidence shall be documented and retained.

Crisis-management, emergency and business-continuity arrangements shall be exercised at planned intervals and after significant changes where appropriate. Exercise and incident lessons shall be assigned, monitored and considered during Management Review.

### 3.11 Complaints, Whistleblowing and Remedy

Employees, contractors, clients, affected communities and other stakeholders shall have access to complaints, grievance and whistleblowing mechanisms that are accessible, confidential and protected from retaliation. Anonymous reporting shall be accepted through the routes published by Castor Vali.

Complaints and concerns shall be assessed, investigated and escalated in accordance with their seriousness. Where Castor Vali has caused or contributed to an adverse impact, the company shall cooperate in or provide appropriate remedy or redress. Criminal conduct, human-rights violations or imminent danger shall be escalated immediately to the COO or another appropriate C-Suite member and notified externally where required.

### 3.12 Documented Information

Documents and records necessary to plan, deliver, monitor and demonstrate control of security operations shall be created, approved, protected, retained and disposed of in accordance with Castor Vali's document-control and retention arrangements. Records shall be accurate, legible, traceable and accessible to authorised persons.

Operational records from country operations, suppliers and subcontractors shall be captured within the appropriate controlled location. Sensitive personnel, client, security, investigation and human-rights information shall be protected according to its classification and applicable data-protection and confidentiality requirements.

## 4 Monitoring and Enforcement

Conformity with this Policy and the effectiveness of the Security Operations Management System shall be monitored through performance indicators, operational oversight, incident and complaint data, client and stakeholder feedback, supplier monitoring, exercises, compliance evaluations, internal audits and Management Review.

Nonconformities shall be controlled and corrected, their consequences addressed and their root causes and potential wider extent evaluated. Corrective and preventive actions shall be assigned, completed, verified

for effectiveness and recorded. Relevant policies, procedures, risk assessments, training and controls shall be updated where necessary.

Failure to comply with this Policy may result in suspension or removal from a task, disciplinary action, contractual action, supplier corrective action or termination of the relevant relationship, subject to applicable law and contractual requirements.

## 5 Policy Review and Updates

The COO is responsible for ensuring that this Policy is reviewed in accordance with the Management Review Schedule and whenever there is:

- a significant change to Castor Vali's strategy, services, structure or operating context;
- a material change in applicable law, licensing, contractual or voluntary commitments;
- a significant security incident, human-rights allegation, complaint or investigation finding;
- a material change in risk, threat intelligence, suppliers, subcontractors or host-nation security arrangements;
- an audit finding or evidence that the Policy or management system is ineffective; or
- a relevant change to ISO 18788, ISO 28007 or another applicable management-system requirement.

Updates shall be approved, controlled and communicated in accordance with the Integrated Management System. This Policy shall remain available as documented information, be communicated to appropriate persons working for or on behalf of Castor Vali, be available to relevant stakeholders and be visibly endorsed by top management.

**Policy approved by:** **Steve Grant**
**CEO**
**Castor Vali Group**