SURKOVSKY CENTRE LTD

RISK MANAGEMENT POLICY
Risk Governance, Assessment and Management Framework

Document Number:	RM-001
Document Title:	Risk Management Policy
Document Classification:	Internal Governance Document
Company:	Surkovsky Centre Ltd
Registered Office:	London, United Kingdom
Version:	1.0
Effective Date:	1 August 2026
Document Owner:	Director
Approved By:	Board of Directors
Review Period:	Every 12 months
Document Status:	Approved

Document Control

Document No.	Version	Issue Date	Review Date
RM-001	1.0	1 August 2026	1 August 2027

Ano. Uděláme **RM-001 – Risk Management Policy** přesně v té struktuře, kterou jsem navrhl, a ve stejném profesionálním formátu jako vaše ostatní dokumenty.

Ještě jsem ověřil aktuálnost podkladů: **ISO 31000:2018 je stále platná publikovaná verze**, přestože se již připravuje její třetí vydání. ISO ji uvádí jako současnou publikovanou normu; nová verze je zatím pouze ve vývoji. **HM Treasury Orange Book** byl skutečně aktualizován **29 July 2026** a jeho současná struktura zdůrazňuje governance, integraci řízení rizik, identifikaci a hodnocení, treatment, monitoring, reporting a continual improvement.

Začátek dokumentu bych tedy napsal takto:

SURKOVSKY CENTRE LTD

RISK MANAGEMENT POLICY

Risk Governance, Assessment and Management Framework

Document Information

Document Number	RM-001
Document Title	Risk Management Policy

Document Information

Company	Surkovsky Centre Ltd
Registered Office	London, United Kingdom
Version	1.0
Effective Date	1 August 2026
Review Date	1 August 2027
Document Owner	Director
Approved By	Director
Document Status	Approved

Document Control

Version	Date	Description	Approved By
1.0	1 August 2026	Initial Issue	Director

---

1. Introduction

Surkovsky Centre Ltd recognises that effective risk management is an essential component of sound governance, responsible decision-making and the achievement of the Company's strategic and operational objectives.

Risk is inherent in all organisational activities and may arise from internal or external events, decisions, circumstances or uncertainties. Effective risk management does not seek to eliminate all risk. Rather, it provides a structured and proportionate framework for identifying, assessing, evaluating, treating, monitoring and communicating risks so that informed decisions can be made and the Company's objectives can be pursued responsibly.

Surkovsky Centre Ltd is committed to integrating risk management into its governance, planning, decision-making and operational activities. The approach adopted by the Company is proportionate to its size, structure, activities and operating environment.

This Policy establishes the principles, responsibilities and processes through which risks affecting Surkovsky Centre Ltd are identified, assessed, managed, monitored and reviewed.

---

2. Purpose

The purpose of this Policy is to establish a consistent and systematic framework for the management of risk across Surkovsky Centre Ltd.

The Policy aims to:

- support the achievement of the Company's strategic and operational objectives;
- promote informed and risk-aware decision-making;
- identify threats and opportunities at an appropriate stage;
- protect the Company's people, assets, information, finances, reputation and activities;
- support compliance with applicable legal, regulatory, contractual and organisational requirements;
- improve organisational resilience and business continuity;
- establish clear responsibilities for the ownership and management of risk;
- ensure that significant risks are appropriately assessed, treated, monitored and reported;
- support the effective allocation of resources;
- encourage learning from incidents, changes and experience; and
- promote continual improvement in the Company's risk management arrangements.

Risk management shall be applied proportionately and shall support, rather than unnecessarily obstruct, legitimate organisational activity, innovation and development.

---

3. Scope

This Policy applies to all activities undertaken by or on behalf of Surkovsky Centre Ltd.

It applies, where relevant, to:

- the Director and any future directors;
- employees;
- contractors and consultants;
- researchers;
- educators and trainers;
- volunteers;
- project participants;
- persons acting on behalf of the Company; and
- third parties where risk management responsibilities arise through contractual or other arrangements.

The Policy applies to strategic, operational, financial, legal, regulatory, compliance, information, cyber security, data protection, people, third-party, educational, research, publishing, business continuity, reputational and other material risks affecting the Company.

Risk management considerations should be incorporated, where proportionate, into significant decisions, projects, contractual arrangements, new activities, partnerships and material changes to existing operations.

---

4. Regulatory and Good Practice Framework

The Company's approach to risk management is informed by recognised risk management principles and good practice, taking account of the nature, scale and complexity of Surkovsky Centre Ltd.

In particular, this Policy has regard to:

ISO 31000:2018 – Risk management — Guidelines

ISO 31000 provides internationally recognised principles, a framework and a process for managing risk. It promotes the integration of risk management into governance, strategy, planning, decision-making and organisational activities.

Surkovsky Centre Ltd uses ISO 31000 as a **good-practice reference framework**. Adoption of this Policy does not constitute or imply certification to ISO 31000.

HM Treasury – The Orange Book: Management of Risk – Principles and Concepts

The Company also has regard, where relevant and proportionate, to the risk management principles contained in HM Treasury's Orange Book.

The Orange Book is primarily directed at UK central government organisations and public bodies. Surkovsky Centre Ltd is a private company and is not represented as being subject to the Orange Book. Relevant principles are used voluntarily as an additional governance and risk-management benchmark where they are appropriate to the Company's circumstances.

The Company may also have regard to applicable legislation, regulatory guidance, contractual requirements, sector-specific guidance and other recognised standards where these are relevant to a particular risk.

Nothing in this Policy replaces or limits any legal or regulatory obligation applicable to the Company.

---

5. Risk Management Principles

Risk management within Surkovsky Centre Ltd shall be based on the following principles.

5.1 Integrated

Risk management should form part of governance, planning, decision-making and normal organisational activity rather than operate as an isolated administrative process.

5.2 Structured and Consistent

Risks should be identified, described, assessed and managed using a consistent methodology that enables meaningful comparison and prioritisation.

5.3 Proportionate

The level of risk management activity should reflect the significance, complexity and potential consequences of the relevant activity or decision.

5.4 Context-Specific

Risk management arrangements should reflect the Company's objectives, organisational structure, operating environment and activities.

5.5 Informed by Available Information

Risk decisions should be based on reliable and relevant information reasonably available at the time, while recognising uncertainty and limitations in available information.

5.6 Inclusive and Consultative

Where appropriate, persons with relevant knowledge, responsibility or expertise should contribute to the identification, assessment and treatment of risks.

5.7 Dynamic

Risk management should respond to changes in the Company's internal and external environment. New and emerging risks should be considered as circumstances develop.

5.8 Consideration of Human and Organisational Factors

Human behaviour, competence, organisational culture, communication and decision-making may influence both the creation and management of risk and should therefore be considered where relevant.

5.9 Continual Improvement

The Company's risk management arrangements should develop through monitoring, experience, incidents, lessons learned and periodic review.

5.10 Creation and Protection of Value

Risk management should contribute to the achievement of the Company's objectives, protection of its resources and reputation, organisational resilience and responsible development.

---

6. Definition of Risk

For the purposes of this Policy, risk is understood as the effect of uncertainty on the achievement of objectives.

Risk may arise from events, circumstances, decisions, actions, omissions, dependencies or changes that may affect the Company's ability to achieve its strategic, operational or other objectives.

Risk may have negative consequences, positive consequences, or a combination of both. Risk management therefore includes consideration of both:

- threats that may adversely affect the Company; and

- opportunities that may support or improve the achievement of the Company's objectives.

A risk should, where practicable, be described in a manner that identifies:

- the source or cause of the risk;
- the uncertain event or circumstance;
- the potential consequences;
- the objectives, activities, persons or assets that may be affected; and
- relevant existing controls.

Risk should not be confused with an issue or incident that has already occurred. Once a risk event has occurred, it should be managed as an incident, issue or other appropriate matter while any continuing or resulting risks remain subject to this Policy.

---

7. Risk Management Objectives

The Company's risk management arrangements are intended to provide reasonable support for effective governance and decision-making rather than absolute protection against uncertainty or loss.

The objectives of risk management are to:

- improve the likelihood of achieving the Company's objectives;
- identify material risks at an appropriate stage;
- enable informed decisions based on an understanding of uncertainty and potential consequences;
- establish appropriate priorities for risk treatment;
- reduce avoidable disruption, loss, harm or non-compliance;
- protect the Company's people, information, finances, assets, activities and reputation;
- identify and consider opportunities where appropriate;
- support organisational resilience and continuity;
- improve the quality and consistency of internal controls;
- support responsible innovation and development;
- provide an appropriate basis for monitoring and reporting significant risks; and
- promote learning and continual improvement.

Risk management shall not be used solely as a mechanism for avoiding risk. The Company recognises that the achievement of legitimate organisational objectives may require the acceptance of an appropriate and proportionate level of risk.

8. Governance and Responsibilities

Risk management is an integral part of the governance arrangements of Surkovsky Centre Ltd.

Responsibility for risk management shall be allocated at a level appropriate to the Company's size, structure and activities.

The Company shall maintain a proportionate governance approach that provides for:

- overall oversight of risk management;
- identification and assessment of material risks;
- allocation of responsibility for individual risks;
- implementation and monitoring of appropriate controls;
- escalation of significant or changing risks;
- maintenance of appropriate risk records;
- periodic review of the Company's risk profile; and
- review and improvement of the risk management framework.

The Company does not consider it necessary to establish a separate Risk Committee unless the scale, complexity or nature of its activities makes such a committee appropriate in the future.

Where specialist knowledge is required, the Company may obtain advice or assistance from appropriately qualified external professionals.

9. Role of the Director

The Director has overall responsibility for the establishment, implementation and oversight of the Company's risk management framework.

The Director is responsible for:

- promoting an appropriate risk-aware culture;
- approving this Policy and material amendments to it;
- determining the Company's overall approach to risk;
- ensuring that material risks are identified and appropriately assessed;
- approving the Company's risk assessment methodology;
- determining or approving risk appetite and tolerance where appropriate;
- reviewing significant and critical risks;
- ensuring that appropriate risk treatments and controls are implemented;
- determining whether significant residual risks may be accepted;

- ensuring that material changes in the Company's activities or operating environment are considered from a risk perspective;
- ensuring that the Risk Register is maintained and periodically reviewed;
- considering emerging risks;
- ensuring appropriate escalation and response to serious risk events;
- considering lessons arising from incidents and control failures; and
- periodically reviewing the effectiveness and proportionality of the Company's risk management arrangements.

As the Company develops, specific risk management responsibilities may be delegated to other directors, employees, managers, project leads, advisers or other appropriate persons.

Delegation of responsibility does not remove the Director's overall governance responsibility for the Company's risk management framework.

---

10. Risk Ownership

Each material risk recorded in the Company's Risk Register should have an identified Risk Owner.

A Risk Owner is the person with primary responsibility for ensuring that a particular risk is appropriately understood, assessed, monitored and managed.

The Risk Owner should have sufficient knowledge of the relevant activity and, where practicable, sufficient authority to coordinate or implement appropriate risk management actions.

The responsibilities of a Risk Owner may include:

- reviewing the description and assessment of the risk;
- identifying and evaluating existing controls;
- proposing or implementing additional risk treatments;
- monitoring relevant risk indicators and changes;
- ensuring agreed actions are completed;
- reporting significant changes in exposure;
- escalating risks that exceed approved tolerance or require higher-level decisions; and
- supporting periodic review of the Risk Register.

For risks that affect the Company as a whole, the Director may act as the Risk Owner.

Risk ownership does not mean that the Risk Owner is personally responsible for causing the risk or for carrying out every control associated with it.

---

11. Risk Identification

Risk identification is the structured process of recognising and describing uncertainties that may affect the achievement of the Company's objectives.

Risks should be identified in relation to the Company's objectives, activities, decisions, projects, resources, dependencies and operating environment.

Risk identification should consider both internal and external sources of risk.

11.1 Internal Sources

Internal sources may include, where relevant:

- governance and decision-making;
- people and competence;
- dependence on key individuals;
- internal processes and procedures;
- financial resources;
- information and records;
- information technology;
- cyber security;
- data protection;
- physical and digital assets;
- project management;
- internal controls;
- organisational change;
- research and educational activities;
- publishing activities;
- communication; and
- business continuity arrangements.

11.2 External Sources

External sources may include, where relevant:

- changes in legislation or regulation;
- economic conditions;
- technological change;
- cyber threats;

- suppliers and service providers;
- contractual counterparties;
- infrastructure disruption;
- market conditions;
- social or demographic developments;
- geopolitical developments;
- public health events;
- severe weather or other environmental events;
- changes in stakeholder expectations; and
- other external events outside the Company's direct control.

11.3 Sources of Information

Risk identification may draw upon:

- strategic and operational planning;
- previous incidents and near misses;
- complaints and feedback;
- internal reviews;
- audits or external assessments;
- contractual requirements;
- regulatory or legislative developments;
- information from suppliers and service providers;
- relevant professional or sector guidance;
- business impact analysis;
- project planning;
- changes in the Company's activities;
- lessons learned;
- scenario analysis; and
- professional judgement.

Risks should be identified regardless of whether their source is within the Company's direct control.

Risk identification shall be an ongoing process and should not be limited to the annual review of the Risk Register.

12. Risk Categories

To support systematic identification and reporting, the Company may classify risks into appropriate categories.

The categories provide a framework for identifying risks and should not be treated as an exhaustive or restrictive list.

The principal categories used by Surkovsky Centre Ltd may include:

12.1 Strategic Risk

Risks affecting the Company's strategic direction, objectives, development, priorities or long-term sustainability.

12.2 Governance Risk

Risks arising from governance arrangements, decision-making, accountability, oversight or organisational structure.

12.3 Operational Risk

Risks arising from processes, systems, resources or the day-to-day delivery of the Company's activities.

12.4 Financial Risk

Risks affecting financial resources, income, expenditure, cash flow, banking, financial controls or the financial sustainability of the Company.

12.5 Legal and Regulatory Risk

Risks arising from failure to comply with applicable legislation, regulations, legal obligations or regulatory requirements.

12.6 Compliance and Ethical Risk

Risks relating to internal policies, professional standards, ethical requirements, integrity, bribery, corruption, conflicts of interest or other compliance obligations.

12.7 Information and Data Protection Risk

Risks affecting the confidentiality, integrity, availability, lawful processing, retention or protection of information and personal data.

12.8 Cyber Security and Technology Risk

Risks arising from cyber threats, unauthorised access, malicious activity, system failure, technological dependency, software or hardware failure, or loss of digital services.

12.9 People and Key-Person Risk

Risks relating to availability, competence, capacity, conduct, health and safety, succession or dependency on individuals who perform important functions.

12.10 Third-Party and Supplier Risk

Risks arising from suppliers, contractors, consultants, technology providers, professional advisers, partners or other external dependencies.

12.11 Educational Risk

Risks associated with educational activities, training, academic standards, learner experience, educational materials or delivery arrangements.

12.12 Research Risk

Risks associated with research activities, research integrity, ethics, methodology, data, publication or research collaboration.

12.13 Publishing and Intellectual Property Risk

Risks associated with publishing activities, copyright, intellectual property, licensing, authorship, content or distribution.

12.14 Business Continuity and Resilience Risk

Risks that may cause significant interruption to critical activities, systems, services, resources or organisational capabilities.

12.15 Reputational Risk

Risks that may adversely affect confidence in, or the reputation and credibility of, Surkovsky Centre Ltd.

12.16 Project and Change Risk

Risks associated with projects, implementation of new systems or activities, organisational change, deadlines, resources or delivery objectives.

A single risk may fall within more than one category. The purpose of categorisation is to support identification, analysis and oversight rather than to force each risk into a single classification.

---

13. Risk Assessment Methodology

Once identified, risks shall be assessed using a structured and proportionate methodology.

The assessment should consider:

1. the nature and causes of the risk;
2. the potential consequences;
3. the likelihood of the risk occurring;
4. the potential impact on the Company or its objectives;
5. existing controls;
6. the effectiveness of those controls;

7. the resulting residual risk;
8. the Company's risk appetite or tolerance, where applicable; and
9. whether further treatment is required.

The Company's standard quantitative assessment methodology uses a five-point scale for **Likelihood** and a five-point scale for **Impact**.

The basic risk score is calculated as:

Risk Score = Likelihood × Impact

The resulting score ranges from **1 to 25**.

The numerical score supports consistent assessment and prioritisation but shall not replace professional judgement. Particular attention may be required where a risk has potentially severe legal, safety, financial, data protection, ethical or reputational consequences even where its likelihood is assessed as low.

The Company shall assess both inherent and residual risk where this is proportionate and useful.

---

14. Likelihood Assessment

Likelihood represents the estimated probability or frequency of a risk event occurring within the relevant assessment period.

Unless another assessment period is more appropriate for a particular risk, likelihood should normally be considered in the context of the Company's current activities and planning horizon.

The following five-point scale shall normally be used:

Score	Rating	General Description
1	Rare	The event is highly unlikely to occur.
2	Unlikely	The event could occur but is not expected under normal circumstances.
3	Possible	The event may occur and there is a credible possibility of occurrence.
4	Likely	The event is expected to occur in a number of circumstances or has occurred with some regularity.
5	Almost Certain	The event is expected to occur or is already occurring frequently.

Likelihood assessments should take account, where relevant, of:

- historical experience;
- previous incidents and near misses;
- existing controls;

- changes in circumstances;
- exposure to the source of risk;
- external evidence;
- professional judgement;
- dependencies;
- known vulnerabilities; and
- uncertainty in the available information.

Where reliable numerical probability data are available, they may supplement the qualitative assessment.

---

15. Impact Assessment

Impact represents the potential severity of the consequences if the risk event occurs.

Impact should be considered across all relevant dimensions rather than solely in financial terms.

Relevant consequences may include:

- strategic impact;
- operational disruption;
- financial loss;
- legal or regulatory consequences;
- data or information loss;
- harm to individuals;
- interruption of educational or research activities;
- contractual consequences;
- reputational damage;
- loss of stakeholder confidence; and
- interruption of critical services or activities.

The following five-point scale shall normally be used:

Score	Rating	General Description
1	Insignificant	Minimal effect; readily manageable within normal activities.
2	Minor	Limited disruption or loss requiring routine management attention.

3	Moderate	Material impact requiring specific management action and potentially affecting an important activity or objective.
4	Major	Serious impact affecting significant activities, obligations, resources or organisational objectives and requiring senior management attention.
5	Severe / Critical	Very serious or potentially sustained impact threatening critical activities, significant legal or regulatory obligations, financial sustainability, important information, individuals or the Company's ability to achieve key objectives.

Where a risk could produce several types of impact, the assessment should normally reflect the **highest reasonably credible material impact**, taking account of the circumstances and available information.

The Company should avoid understating a risk merely because one dimension of its potential impact is limited.

---

16. Risk Rating and Risk Matrix

The standard risk rating is determined by multiplying the Likelihood score by the Impact score.

Risk Rating = Likelihood × Impact

The Company's standard 5 × 5 Risk Matrix is:

Likelihood ↓ / Impact →	**1 Insignificant**	**2 Minor**	**3 Moderate**	**4 Major**	**5 Severe / Critical**
5 Almost Certain	5	10	15	20	25
4 Likely	4	8	12	16	20
3 Possible	3	6	9	12	15
2 Unlikely	2	4	6	8	10
1 Rare	1	2	3	4	5

For management and reporting purposes, scores shall normally be classified as:

Score	**Risk Level**	**General Management Response**
1–4	Low	Manage through routine controls and periodic monitoring.
5–9	Moderate	Monitor and consider whether additional controls or treatment are proportionate.

10–16	High	Active management and documented treatment should normally be required. The risk should receive appropriate management attention.
17–25	Critical	Immediate or priority management attention is required. Treatment, escalation and close monitoring should normally be undertaken.

Risk ratings provide a decision-support mechanism. They do not automatically determine whether a particular activity must proceed, cease or be modified.

The Director may determine that a risk requires a higher level of attention than its numerical score alone would indicate where the potential consequences, uncertainty, legal obligations or strategic significance justify such treatment.

---

17. Inherent Risk

Inherent Risk is the level of risk that would exist before taking account of specific controls or risk treatments designed to manage that risk.

Assessment of inherent risk helps the Company understand the underlying exposure and the significance of the controls upon which it relies.

Where proportionate, the Risk Register should record:

- inherent likelihood;
- inherent impact; and
- inherent risk score.

The assessment should represent a reasonable view of the risk in the absence of relevant controls rather than an unrealistic worst-case scenario.

---

18. Existing Controls

Existing Controls are measures already in place that prevent, reduce, detect, respond to or otherwise modify a risk.

Controls may include:

- policies and procedures;
- approvals and authorisations;
- segregation or allocation of responsibilities;
- contractual protections;
- financial controls;
- access controls;
- backups and recovery arrangements;

- cyber security measures;
- training and competence requirements;
- monitoring and review;
- insurance;
- professional advice;
- physical security;
- quality assurance arrangements;
- contingency arrangements; and
- other preventive, detective or corrective measures.

The existence of a control does not automatically mean that the risk is adequately managed.

When assessing controls, consideration should be given to whether they are appropriately designed, implemented, operating as intended and proportionate to the risk.

---

19. Residual Risk

Residual Risk is the level of risk remaining after taking account of existing controls and their effectiveness.

Residual risk should be assessed using the same Likelihood and Impact methodology used for inherent risk.

Where appropriate, the Risk Register should therefore distinguish between:

Inherent Risk → Existing Controls → Residual Risk

The residual risk assessment provides the principal basis for determining whether:

- the risk is within an acceptable level;
- further treatment is required;
- the risk should be escalated;
- the activity should be modified or avoided; or
- the remaining risk may be formally accepted.

Residual risk can never be assumed to be zero merely because controls have been implemented.

---

20. Risk Appetite and Tolerance

Risk appetite represents the amount and type of risk that the Company is prepared to accept in pursuit of its objectives.

Risk tolerance represents the acceptable level of variation or exposure around particular objectives, activities or risk categories.

Surkovsky Centre Ltd recognises that its appetite for risk may differ according to the nature of the activity.

The Company may accept proportionate levels of risk where doing so supports legitimate development, innovation, research, education, publishing, partnership or other organisational objectives.

The Company shall normally have a **low or very low appetite** for risks that could result in:

- unlawful activity;
- bribery, corruption, fraud or deliberate misconduct;
- serious breaches of data protection or confidentiality obligations;
- serious harm to individuals;
- significant breaches of legal or regulatory requirements;
- deliberate compromise of research or academic integrity; or
- conduct fundamentally inconsistent with the Company's ethical standards.

Risk appetite shall not override legal or regulatory requirements.

Where uncertainty exists as to whether a significant risk falls within acceptable tolerance, the matter should be referred to the Director for determination.

---

21. Risk Treatment

Risk treatment is the process of selecting and implementing measures to modify risk.

Where a risk is assessed as requiring further action, the Company shall determine an appropriate treatment having regard to:

- the nature and significance of the risk;
- the Company's objectives;
- the likelihood and potential impact of the risk;
- existing controls and their effectiveness;
- legal, regulatory, contractual and ethical obligations;
- the Company's risk appetite and tolerance;
- the cost, practicality and effectiveness of additional measures;
- available resources;
- potential unintended consequences; and
- the residual risk expected after treatment.

Risk treatment may involve one or more of the following approaches:

- accepting the risk;
- avoiding the risk;
- reducing the likelihood or impact of the risk;
- removing or modifying the source of the risk;
- transferring or sharing elements of the risk; or
- pursuing an opportunity while managing associated risk.

Risk treatment decisions should be proportionate and documented where the risk is material.

Where additional treatment is required, the Company should identify, as appropriate:

- the proposed action;
- the person responsible;
- the target completion date;
- required resources;
- the intended outcome;
- the expected residual risk; and
- arrangements for monitoring implementation.

Implementation of a treatment does not remove the need to monitor the risk.

---

22. Risk Acceptance

Risk acceptance means making an informed decision to retain a risk without introducing further treatment beyond existing controls.

A risk may be accepted where:

- the residual risk is within the Company's risk appetite or tolerance;
- further treatment would be disproportionate to the potential benefit;
- effective additional treatment is not reasonably available;
- the risk is necessary to pursue a legitimate organisational objective;
- the cost or consequences of further treatment would exceed the reasonably expected benefit; or
- the Director determines that acceptance is appropriate having regard to all relevant circumstances.

Acceptance of risk shall not be used to avoid compliance with legal, regulatory, contractual or other mandatory obligations.

Material accepted risks should remain subject to appropriate monitoring and review.

High or Critical risks should not normally be accepted without explicit consideration and approval by the Director.

---

23. Risk Avoidance

Risk avoidance involves deciding not to commence, or deciding to discontinue, an activity that gives rise to an unacceptable risk.

Avoidance may be appropriate where:

- the potential consequences are unacceptable;
- the risk cannot reasonably be reduced to an acceptable level;
- the activity would expose the Company to unlawful or unethical conduct;
- adequate controls cannot be implemented;
- the expected benefit does not justify the exposure; or
- continuation would be inconsistent with the Company's objectives, obligations or risk appetite.

Risk avoidance should not be applied automatically merely because an activity involves uncertainty.

The Company recognises that excessive avoidance of risk may prevent innovation, development and achievement of legitimate objectives.

---

24. Risk Reduction

Risk reduction involves implementing measures designed to reduce the likelihood, impact, or both, of an identified risk.

Risk reduction measures may include:

- strengthening policies and procedures;
- introducing additional approvals or controls;
- improving training or competence;
- improving cyber security;
- improving backup and recovery arrangements;
- reducing dependency on individual persons or systems;
- introducing alternative suppliers or service arrangements;
- improving contractual protections;
- strengthening financial controls;

- increasing monitoring;
- improving physical or information security;
- introducing contingency arrangements;
- improving quality assurance;
- changing the design or delivery of an activity; or
- obtaining specialist professional advice.

Risk reduction measures should be proportionate to the significance of the risk and should not impose unnecessary administrative or financial burdens where these would provide little additional protection.

---

25. Risk Transfer or Sharing

Certain elements of risk may be transferred or shared with another party where appropriate.

Mechanisms may include:

- insurance;
- contractual allocation of responsibility;
- outsourcing;
- indemnities;
- warranties;
- partnerships;
- specialist service providers; or
- other appropriate arrangements.

Transfer or sharing of risk does not necessarily eliminate the Company's exposure.

The Company may retain legal, regulatory, financial, operational or reputational consequences even where responsibility for particular activities has been contractually allocated to another party.

The Company should therefore assess the capability, reliability and suitability of relevant third parties and monitor material dependencies where appropriate.

No contractual arrangement shall be treated as transferring obligations that cannot lawfully be transferred.

---

26. Risk Register

Surkovsky Centre Ltd shall maintain a **Risk Register** as the principal record of material risks identified and assessed under this Policy.

The Risk Register is intended to provide a clear and proportionate overview of the Company's significant risk exposure and the measures used to manage it.

The Risk Register should, where appropriate, record:

Field	Purpose
Risk ID	Unique reference number
Risk Category	Classification of the risk
Risk Title	Concise identification of the risk
Risk Description	Cause, event and potential consequences
Risk Owner	Person responsible for oversight
Inherent Likelihood	Likelihood before controls
Inherent Impact	Impact before controls
Inherent Risk Score	Likelihood × Impact
Existing Controls	Measures already in place
Control Effectiveness	Assessment of existing controls
Residual Likelihood	Likelihood after controls
Residual Impact	Impact after controls
Residual Risk Score	Remaining risk exposure
Risk Level	Low, Moderate, High or Critical
Further Treatment / Actions	Additional measures required
Action Owner	Person responsible for action
Target Date	Expected completion date
Status	Current position
Review Date	Date for reassessment

The level of detail recorded should be proportionate to the significance and complexity of the risk.

The Risk Register shall not be treated as a static document. It should be updated where:

- a material new risk is identified;
- an existing risk materially changes;

- significant controls are introduced or removed;
- a relevant incident occurs;
- a significant project or activity begins or ends;
- the external operating environment materially changes; or
- a scheduled review identifies a need for amendment.

The Director shall have overall responsibility for ensuring that the Company's Risk Register is maintained and periodically reviewed.

---

27. Emerging Risks

The Company recognises that not all significant risks will be known or fully understood in advance.

Emerging risks are risks that are new, changing, increasing in significance or insufficiently understood and that may materially affect the Company in the future.

Sources of emerging risk may include:

- new technologies;
- artificial intelligence and automation;
- cyber security developments;
- changes in legislation or regulation;
- economic developments;
- changes in educational or research practices;
- changes in publishing and intellectual property environments;
- geopolitical developments;
- changes in suppliers or digital platforms;
- new forms of fraud or misconduct;
- environmental or infrastructure developments; and
- significant changes in the Company's own activities.

The Company should maintain reasonable awareness of developments relevant to its activities and consider whether newly identified uncertainties should be incorporated into the Risk Register.

Emerging risks may initially be difficult to quantify. Lack of complete information shall not prevent the Company from recording, monitoring or responding to a potentially significant risk.

---

28. Strategic and Operational Risks

The Company shall identify and manage strategic and operational risks that could materially affect the achievement of its objectives or the delivery of its activities.

Strategic risks may include risks associated with:

- organisational direction and priorities;
- significant business decisions;
- development of new activities;
- sustainability of operations;
- partnerships and collaborations;
- changes in demand or operating environment;
- concentration of activities or dependencies; and
- failure to adapt to material external change.

Operational risks may include:

- failure or inadequacy of internal processes;
- loss or interruption of critical systems;
- administrative error;
- inadequate documentation;
- insufficient resources;
- failure of operational controls;
- disruption to services or activities;
- project delivery failures; and
- dependency on particular systems, persons or providers.

Strategic and operational risks should be considered when significant new activities, projects or organisational changes are proposed.

---

29. Financial Risks

Financial risks are risks that may adversely affect the Company's financial resources, controls, obligations or sustainability.

Relevant risks may include:

- insufficient liquidity or cash flow;
- unexpected expenditure;
- loss of income;
- banking disruption;

- payment fraud;
- inaccurate financial records;
- unauthorised transactions;
- inadequate financial controls;
- dependency on a limited number of income sources;
- foreign exchange exposure where relevant;
- tax or accounting errors;
- failure of a financial service provider; and
- financial consequences arising from contractual or legal obligations.

The Company shall maintain financial controls proportionate to its size, activities and financial exposure.

Material financial risks should be reflected in the Risk Register where appropriate.

---

30. Legal, Regulatory and Compliance Risks

The Company shall identify and manage material risks arising from applicable legal, regulatory, contractual and compliance obligations.

Relevant areas may include:

- company law;
- taxation and accounting requirements;
- data protection and privacy;
- employment and contractor arrangements;
- intellectual property;
- copyright and licensing;
- contractual obligations;
- anti-bribery and corruption requirements;
- equality and non-discrimination obligations;
- health and safety where applicable;
- research and educational obligations; and
- other legislation or regulatory requirements relevant to the Company's activities.

The Company shall seek appropriate professional advice where a matter involves significant legal, regulatory, tax, accounting or specialist uncertainty.

Compliance risks shall not be accepted merely because the likelihood of enforcement or detection is considered low.

---

31. Information, Cyber and Data Risks

Information is an important organisational asset and shall be subject to proportionate protection.

The Company shall consider risks affecting the:

- **confidentiality** of information;
- **integrity** and accuracy of information; and
- **availability** of information and systems.

Relevant risks may include:

- unauthorised access;
- cyber attack;
- malware or ransomware;
- phishing and social engineering;
- account compromise;
- loss or theft of devices;
- accidental deletion;
- corruption or loss of data;
- inadequate backups;
- failure of cloud or hosting services;
- inappropriate disclosure;
- loss of access credentials;
- software or hardware failure;
- data protection breaches; and
- dependency on third-party technology providers.

Controls should be proportionate to the sensitivity, importance and volume of the information concerned.

Where personal data are involved, risk management shall operate alongside the Company's applicable data protection and privacy arrangements.

---

32. People and Key-Person Risks

The Company shall consider risks arising from dependency on individuals whose knowledge, authority, access or responsibilities are important to the continuity and effectiveness of its activities.

Such risks may include:

- unexpected absence or incapacity;
- loss of specialist knowledge;
- inadequate succession arrangements;
- insufficient capacity;
- lack of necessary competence;
- dependency on a single individual for critical decisions;
- loss of access credentials or information held by one person;
- misconduct or conflict of interest; and
- inability to perform critical responsibilities.

Where a material key-person dependency exists, proportionate measures may include:

- appropriate documentation of critical processes;
- secure arrangements for access to essential records;
- delegation arrangements where appropriate;
- identification of alternative professional or technical support;
- maintenance of current contact and account information;
- contingency arrangements; and
- succession planning proportionate to the Company's circumstances.

The Company recognises that complete elimination of key-person dependency may not be practicable for a small organisation. Such dependency should therefore be identified, understood and managed proportionately.

---

33. Third-Party and Supplier Risks

The Company may depend on external organisations and individuals for technology, professional services, infrastructure, supplies, advice or other activities.

Material third-party risks may include:

- service interruption;
- supplier failure;
- cyber security weaknesses;

- loss or misuse of Company information;
- inadequate service quality;
- financial failure of a supplier;
- breach of contractual obligations;
- legal or regulatory non-compliance;
- concentration of dependency on a single provider; and
- inability to replace a critical service within an acceptable period.

The Company should undertake proportionate due diligence before entering into material third-party arrangements and should consider the criticality of the relevant service.

Where appropriate, controls may include contractual provisions, alternative providers, backups, access arrangements, service monitoring or contingency planning.

---

34. Educational, Research and Publishing Risks

Given the nature of the Company's activities, particular consideration shall be given to risks arising from educational, research and publishing activities.

34.1 Educational Activities

Relevant risks may include:

- inaccurate or inappropriate educational content;
- inadequate quality assurance;
- failure to meet stated educational objectives;
- inappropriate assessment practices;
- disruption to delivery;
- intellectual property issues; and
- reputational consequences arising from educational activities.

34.2 Research Activities

Relevant risks may include:

- research integrity failures;
- ethical concerns;
- inappropriate research methodology;
- inaccurate or unreliable data;
- loss of research data;
- inappropriate authorship or attribution;

- conflicts of interest;
- confidentiality breaches;
- inappropriate use or disclosure of research findings; and
- failure to comply with applicable ethical or contractual requirements.

34.3 Publishing Activities

Relevant risks may include:

- copyright infringement;
- licensing disputes;
- inaccurate attribution;
- publication of unlawful material;
- loss of intellectual property;
- errors in published content;
- contractual disputes; and
- reputational harm.

These risks should be managed in conjunction with the Company's applicable academic integrity, research ethics, quality assurance and other relevant policies and procedures.

---

35. Business Continuity and Resilience Risks

The Company shall identify risks capable of materially disrupting critical organisational activities.

These may include:

- prolonged IT or system failure;
- loss of access to critical information;
- cyber incidents;
- telecommunications failure;
- power or infrastructure disruption;
- failure of a critical supplier;
- loss of access to premises;
- serious data loss;
- unexpected unavailability of key persons;
- significant external disruption; and

- other events affecting the Company's ability to maintain essential activities.

Business continuity risks should be considered in conjunction with the Company's **Business Continuity Policy** and any associated continuity or recovery arrangements.

Priority should be given to identifying:

- critical activities;
- critical information and systems;
- critical dependencies;
- acceptable periods of disruption;
- alternative methods of operation; and
- recovery priorities.

---

36. Reputational Risks

Reputational risk is the risk that an event, conduct, decision or failure may materially damage confidence in, or the credibility and reputation of, Surkovsky Centre Ltd.

Reputational consequences may arise from other risk categories and should therefore be considered as part of the assessment of material risks.

Potential sources may include:

- unethical or inappropriate conduct;
- inaccurate public statements;
- significant service or quality failures;
- legal or regulatory breaches;
- data breaches;
- research or academic integrity failures;
- conflicts of interest;
- bribery, corruption or fraud;
- inappropriate relationships with third parties;
- poor handling of complaints or incidents; and
- misleading representation of the Company's activities, qualifications, status or achievements.

Reputational risk should not be used as a reason to conceal legitimate concerns, incidents or errors.

Where an incident occurs, the Company should prioritise lawful, accurate and responsible action, including appropriate communication and remediation.

37. Risk Escalation

A risk should be escalated to the Director where:

- it is assessed as High or Critical;
- it exceeds an established risk tolerance;
- existing controls appear ineffective;
- the potential consequences have materially increased;
- a significant legal or regulatory issue may arise;
- a serious incident or control failure has occurred;
- urgent resources or decisions are required;
- responsibility for treatment is unclear;
- the risk may materially affect multiple areas of the Company; or
- the Risk Owner considers escalation appropriate.

Critical risks should receive priority consideration.

Escalation should result in a documented decision where proportionate, including whether to:

- introduce additional controls;
- implement contingency measures;
- obtain specialist advice;
- modify or suspend an activity;
- accept the residual risk;
- invoke business continuity arrangements; or
- take another appropriate course of action.

38. Monitoring and Reporting

Risk management is a continuing process.

Material risks shall be monitored at a frequency proportionate to their significance and rate of change.

Monitoring may consider:

- changes in likelihood or impact;
- effectiveness of controls;
- progress against treatment actions;

- incidents and near misses;
- changes in legislation or regulation;
- changes in external circumstances;
- new dependencies;
- emerging threats;
- changes in the Company's activities; and
- relevant performance or risk indicators.

High and Critical risks should normally be reviewed more frequently than Low or Moderate risks.

The Director shall receive or undertake appropriate review of the Company's material risk profile and determine whether further action is required.

Risk reporting should be clear, proportionate and focused on information necessary to support decisions.

---

39. Incident and Lessons-Learned Review

Significant incidents, near misses, control failures or unexpected outcomes should be reviewed where they provide useful information about the Company's risk exposure or controls.

A review may consider:

- what occurred;
- why it occurred;
- which controls operated effectively;
- which controls failed or were absent;
- whether the relevant risk had previously been identified;
- whether the likelihood or impact assessment was appropriate;
- whether the response was effective;
- what corrective action is required; and
- whether similar risks exist elsewhere in the Company.

Relevant lessons should be incorporated into the Risk Register, controls, procedures, training or other organisational arrangements as appropriate.

The purpose of a lessons-learned review is to improve future risk management and organisational resilience.

---

40. Policy Review and Continuous Improvement

This Policy shall normally be reviewed at least annually and may be reviewed earlier where:

- there is a material change in the Company's activities or structure;
- significant new risks emerge;
- relevant legislation or regulatory expectations change;
- a serious incident or control failure occurs;
- experience demonstrates that the existing framework requires improvement; or
- recognised risk management good practice materially changes.

Risk management arrangements shall be developed proportionately as the Company grows or its activities become more complex.

The Company shall seek continual improvement through experience, monitoring, review, professional guidance and lessons learned.

---

41. Related Company Documents

This Policy should be read, where applicable, alongside relevant Company documents, including:

- **GOV-001 – Code of Conduct**
- **GOV-002 – Equality, Diversity & Inclusion**
- **GOV-003 – Governance Structure**
- **RES-001 – Research Ethics Policy**
- **EDU-001 – Academic Integrity Policy**
- **QA-001 – Quality Assurance Policy**
- **ABC-001 – Anti-Bribery and Corruption Policy**
- **POL-001 – Privacy Policy**
- **POL-002 – Data Protection Policy**
- **Business Continuity Policy**
- **Complaints Procedure**
- **Risk Register**
- and other applicable policies, procedures and governance documents.

Where there is any inconsistency between this Policy and an applicable legal or regulatory requirement, the applicable legal or regulatory requirement shall take precedence.

---

42. Approval

This Risk Management Policy has been approved by the Director of Surkovsky Centre Ltd.

The Policy takes effect on **1 August 2026** and shall remain in force until amended, replaced or withdrawn.

The Director is responsible for ensuring that this Policy is implemented and reviewed in accordance with its provisions.

Approved by: Director
Surkovsky Centre Ltd

Signature:

Name: Jozef SURKOVSKY

Date: 1 August 2026

Document History

Version	Date	Description	Approved By
1.0	1 August 2026	Initial issue	Director

End of Document