[Company name]

How to use this document: delete this paragraph before saving, sharing, or circulating it. Every part shown in blue is yours to replace: type your own details over each blue [field] until no blue remains. Then select all (Ctrl+A) and set the font colour to the same dark colour throughout. What is left is your finished document.

Risk Management Policy

[Company name] This policy sets out how [Company name] identifies, assesses, and manages risk. It applies to everyone who works for [Company name], including directors, managers, employees, and [Other people covered, e.g. contractors and volunteers]. Good risk management helps [Company name] meet its aims, protect its people and assets, and make better decisions.

1. Purpose and scope. Risks to the aims of [Company name] must be identified early; managers assess and respond to risk in one clear, consistent way; every risk and response has a named owner; and important risks reach the board in good time. This policy covers all activities of [Company name], including its offices at [Office location], its services, projects, finances, information and systems, and its work with [External parties, e.g. suppliers, partners, and customers], and applies to all departments, including [Department name] and [Department name].

2. Definitions. Risk: an uncertain event that, if it happens, would affect the aims of [Company name]. Risk appetite: the amount and type of risk [Company name] is willing to accept in pursuit of its aims. Risk owner: the person named as responsible for managing a named risk. Control: a measure put in place to reduce the likelihood or the impact of a risk. Residual risk: the risk that remains after controls have been put in place.

3. Risk appetite. The board of [Company name] has agreed the appetite below, reviewed at least once a year, or sooner if the circumstances of [Company name] change. Any risk outside the agreed appetite must be escalated to [Name or role, e.g. the chief executive] and, where needed, to the board.
Financial risk: [Low / Medium / High], [Notes, e.g. the organisation will not accept risks that threaten its ability to pay its debts]
Health and safety: [Low / Medium / High], [Notes, e.g. no appetite for risks to the safety of staff or visitors]
Reputation: [Low / Medium / High], [Notes]
Compliance and legal: [Low / Medium / High], [Notes]
Operational delivery: [Low / Medium / High], [Notes]
Growth and new services: [Low / Medium / High], [Notes]

4. Responsibilities.
Board of directors: sets the risk appetite, reviews the risk register, and holds senior managers to account for risk management.
[Chief executive]: owns this policy, makes sure it is followed, and reports the most important risks to the board.
[Senior manager]: makes sure risks in their area are identified, assessed, and recorded, and that controls are in place.
Risk owner: manages a named risk, reviews its controls, and reports changes to [Name or role].
All employees: report new risks and near misses to their manager, and follow the controls that apply to their work.
[Internal audit or reviewer]: reviews how well this policy is working and reports findings to [Name or role].

5. How risks are managed. Step 1, Identify: risks are identified through [Methods, e.g. team discussions, incident reports, audits, and horizon scanning]; any employee who spots a new risk tells their manager, who records it in the risk register. Step 2, Assess: each risk is scored for likelihood and impact on the scale below; the score is likelihood multiplied by impact, and a score of [Threshold score] or above is a high risk and must be escalated.
1 Rare, negligible effect on [Company name]; 2 Unlikely, minor effect, easily managed; 3 Possible, moderate effect on services or finances; 4 Likely, major effect on services, finances, or reputation; 5 Almost certain, severe effect, threatening the aims of [Company name].

Step 3, Respond: for each risk the risk owner chooses one response and records it in the risk register: Avoid, stop the activity that creates the risk; Reduce, put controls in place to lower the likelihood or the impact; Transfer, pass some of the risk to another party, for example through insurance or a contract; Accept, accept the risk where it is within the agreed appetite and the cost of control would be greater than the benefit. **Step 4, Monitor and review:** risk owners review their risks at least every [Review period, e.g. three months] and after any incident. The risk register is reviewed by [Name or role] every [Review period] and by the board at least once a year.

6. Risk register. All identified risks are recorded in the risk register of [Company name]. Each entry includes:
Risk reference: [Risk reference, e.g. R-001] Risk description: [Description of the risk and its cause]
Risk owner: [Name of risk owner] Likelihood (1-5): [Score] Impact (1-5): [Score]
Overall score: [Likelihood multiplied by impact] Response: [Avoid / Reduce / Transfer / Accept]
Controls in place: [Controls] Review date: [Review date]

7. Escalation. A risk must be escalated to [Name or role] without delay if its overall score is [Threshold score] or above, it falls outside the agreed risk appetite, a control has failed or an incident has happened, or it affects more than one department or needs a decision the risk owner cannot make.

8. Reporting a new risk. To report a new risk, tell your manager or send the details to [Name or role] at [Email address], including what the risk is, what could cause it, what effect it could have, and any controls already in place. **9. Review and approval.** This policy was approved by the board of [Company name] on [Approval date] and will be reviewed by [Review date], or sooner if the law, the structure, or the activities change. The owner of this policy is [Name of policy owner], [Job title].
Approved by: [Name of approver], [Job title], Signature _____, Date [Date]
Policy owner: [Name of policy owner], [Job title], Signature _____, Date [Date]