IT RISK MANAGEMENT POLICY

StartFast Tech

Document Ref: SFT-RISK-POL-001 | Version: 1.1 | Classification: CONFIDENTIAL

Version Control

Version	Date	Author	Description	Status
1.0	22 Feb 2023	A. Obi (Head of Security)	Initial policy drafted for ISO 27001 certification scope.	Approved
1.1	14 Jun 2023	A. Obi (Head of Security)	Added board reporting section. Risk appetite statement revised.	Approved

Approval and Sign-Off

Role	Name	Signature	Date
Chief Executive Officer	C. Eze	_____	14 Jun 2023
Head of Security	A. Obi	_____	14 Jun 2023
Chief Financial Officer		_____	
Board — Risk & Audit Committee		_____	
Legal Counsel		_____	
Head of Engineering	T. Bello	_____	14 Jun 2023

GAPS: (1) CFO sign-off is absent — financial risk owners have not approved the risk management framework. (2) Board/Audit Committee sign-off is absent. The policy requires board approval of high and critical risk acceptances, yet the board has not approved the policy that establishes this requirement. (3) Legal Counsel sign-off is absent despite regulatory risk (ISO 27001 audit scope, potential NDPA obligations) being within scope.

1. Purpose

This policy defines StartFast Tech's ("StartFast" or "the Company") approach to identifying, assessing, treating, and monitoring IT and information security risks. It supports the Company's ISO 27001 Information Security Management System (ISMS) and satisfies the risk management requirements of ISO 27001:2022 Clause 6.1 and ISO 31000:2018. Effective risk management enables the Company to make informed decisions about accepting or treating risk in pursuit of its growth objectives.

2. Scope

This policy applies to all IT and information security risks affecting StartFast's SaaS platform, corporate infrastructure, customer data, and third-party relationships. It applies to all employees, contractors, and systems within the ISO 27001 certification scope.

> **AUDIT NOTE — DELIBERATE GAP**
> *SCOPE GAP: The ISO 27001 certification scope has not yet been formally determined (it is "under review" per the company description). Risks outside the eventual certification scope may not be subject to this policy, creating potential blind spots in the risk management framework.*

3. Risk Identification

IT risks must be identified through a combination of:

- Annual information security risk assessment led by the Head of Security
- Vulnerability scanning and penetration testing results (quarterly)
- Internal audit and control testing findings
- Supplier and third-party risk assessments
- Incident post-mortem reviews
- Threat intelligence monitoring

> **AUDIT NOTE — DELIBERATE GAP**
> *IDENTIFICATION GAPS: (1) Business stakeholders are not required to participate in risk identification — risks may be identified solely from an IT/security perspective, missing business context and impact. (2) No process for capturing emerging risks from external intelligence sources (e.g. CERT advisories, industry threat reports). (3) "Significant changes" to the business should trigger a risk review — SaaS feature releases, new market entry, and pricing model changes are not mentioned as triggers.*

4. Risk Assessment Methodology

4.1 Risk Scoring

Each identified risk must be assessed using a 5x5 likelihood-impact matrix:

Score	Likelihood	Impact Description
1	Rare (< 5% probability)	Negligible — no material operational or financial impact
2	Unlikely (5–25%)	Minor — limited impact, resolved internally
3	Possible (25–50%)	Moderate — noticeable impact, management attention required
4	Likely (50–75%)	Significant — major operational disruption or financial loss
5	Almost Certain (>75%)	Critical — existential threat to the business

Risk Rating	Score Range	Required Action
Low	1–4	Accept or monitor. Head of Security may accept.
Medium	5–9	Treat or accept with documented rationale. Head of Security may accept.
High	10–16	Treat within 90 days or obtain CEO/Board acceptance. CEO approval required.
Critical	20–25	Immediate treatment plan required. Board acceptance mandatory. Escalate immediately.

4.2 Residual Risk

After controls are applied, the Residual Risk must be assessed using the same scoring matrix. Residual Risk must always be lower than or equal to Inherent Risk — a control that increases risk is not a control.

> **AUDIT NOTE — DELIBERATE GAP**
> *RESIDUAL RISK GAPS: (1) No validation process exists to confirm that stated controls actually reduce risk as claimed — residual scores are self-assessed without independent review. (2) The constraint that Residual <= Inherent is a policy statement but is not enforced technically. Errors in the register where Residual > Inherent have occurred and were not detected until audit. (3) No requirement for control effectiveness testing before residual risk scores are accepted as valid.*

5. Risk Treatment

Each risk must be assigned one of the following treatment options:

Mitigate: Implement controls to reduce likelihood and/or impact to an acceptable level

Accept: Acknowledge the risk within risk appetite; document rationale and approver

Transfer: Transfer risk to a third party via insurance, contract, or outsourcing

Avoid: Cease the activity generating the risk

> **AUDIT NOTE — DELIBERATE GAP**
> *RISK ACCEPTANCE GAPS: (1) No documented process for risk acceptance exists — no form, workflow, or minimum information requirement is specified. Board acceptance of a critical risk requires no specific evidence beyond "board approval." (2) Risk acceptance has no time limit — risks accepted years ago may remain accepted indefinitely without re-review. (3) A risk rated as Critical could theoretically be downgraded to Medium by the Head of Security and self-accepted, bypassing board oversight.*

6. Risk Appetite

StartFast Tech's risk appetite is defined as:

> *"We accept Low and some Medium risks in pursuit of growth objectives, but seek to eliminate High and Critical risks within 12 months of identification. We have zero tolerance for risks that could result in loss of customer data or regulatory non-compliance."*

AUDIT NOTE — DELIBERATE GAP

RISK APPETITE GAPS: (1) "Some Medium risks" is not quantified — how many, of what type, under what conditions, is entirely subjective. (2) No thresholds are defined by risk category (operational, financial, regulatory, reputational). ISO 31000 and ISO 27001 expect category-specific appetite statements. (3) "Zero tolerance for customer data loss" is aspirational rather than operational — no control threshold or KRI is linked to this statement. (4) No Board approval of the risk appetite statement is documented, despite board being the risk appetite setter under governance best practice. (5) No review frequency for the appetite statement is defined — it was last reviewed at policy inception and has not been updated since.

7. Risk Register

The IT Risk Register must be maintained by the Head of Security and reviewed quarterly by the senior leadership team. Risk register updates must be completed within 30 days of the quarterly review. A summary of the register, including all High and Critical risks, must be presented to the Board quarterly.

AUDIT NOTE — DELIBERATE GAP

RISK REGISTER GAPS: (1) The risk register format, required fields, and storage location are not defined in this policy. (2) No minimum content is defined for the board report — risks rated Critical could be summarised without sufficient context for board decision-making. (3) No requirement for the board to formally resolve, acknowledge, or minute the risks presented to them — risks may be presented but not acted upon without consequence.

8. Policy Review

This policy is reviewed annually. Last reviewed: June 2023. Next review: June 2024.