HighTable

[Company]

RISK MANAGEMENT

POLICY

Identification and management of risk

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Risk Management Policy

3.1 Purpose

The purpose of this policy is to set out the risk management policy for the company for information security.

3.2 Scope

All employees and third-party users.

Risk and risk management as applied to information security and the confidentiality, integrity and availability of organisation owned, processed, stored, and transmitted information.

3.3 Principle

Information security management for the company is based on appropriate and adequate risk and risk management.

3.4   What is risk Management

Risk can be defined as the threat or possibility that an action or event will adversely or beneficially affect an organization's ability to achieve its objectives.

███

██

██

3.5   Risk Appetite

Overall, the company has a Moderate Risk appetite meaning risks are mitigated in a cost effective and proportionate manner to the risk and some risk acceptance is acceptable based on business need.

3.5.1 Low Risk Appetite

The company has a low-risk appetite to the following which means that risks will not be accepted and that will have resources allocated to mitigate risk in a proportionate and cost-effective manner:
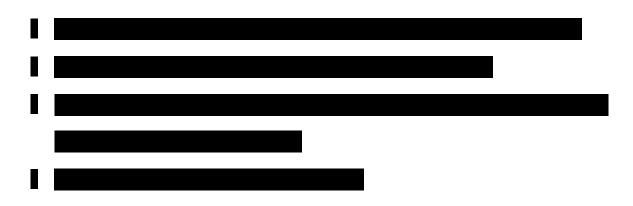
- ██████████████████████████████████████
  ████████
- ███
- ██████████████████████████

3.5.2 Moderate Risk Appetite

The following will most likely have resources allocated to mitigate risk in a proportionate and cost-effective manner:

- ██
- ███████████████████████████████████
- ███
  ███████████████████████
- ███████████████████████████████

3.6   Risk Identification and Assessment

Risks assessments are carried out at regular intervals or at least every 12 months and where there has been or likely to be significant change.

Risks are identified and assessed at least for

- The processing, storing, or transmitting of confidential, personal or card holder information
- Third party suppliers that are processing, storing, or transmitting of confidential, personal or card holder information
- ████████
- ████████████

An ISO 27001 controls risk assessment is carried out at least once every 12 months.

3.7   Risk Register

All risks are recorded in the company risk register.

3.8   Risk Reporting

The risk register is reviewed at the Management Review Team meeting.

Risks are reported to the Management Review Team.

██

██

██

████████

3.9   Risk Review

Risks are regularly reviewed and monitored at the Management Review Team meeting
to ensure:

- Risk action progress

- Risk action effectiveness

- Management of residual risk

3.10   Risk Treatment

All risks are assigned a risk owner

3.10.1 Risk Acceptance

The decision to accept risks is taken by the relevant departmental manager and or senior management.

The criterion for accepting risk is based on

- The risk is categorised as low, and it is not cost effective to treat the risk.

- A business or commercial opportunity exists that outweighs the threat and impact.

- ██████████████████████

█ █████████████████████████████████████

3.10.2 Risk Mitigation

Where a risk is to be mitigated

- A plan of action is approved by the relevant departmental manger and/or the Management Review Team and/or Senior Management.

- ███

█ ███

███████████████████████

3.11   Risk Evaluation

The evaluation of risk impact is considered on impact to

- Compliance and the Law

▮ ███████

▮ █████

▮ ████████████████████

▮ ██████████████

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.