G4 MARKETING GROUP

VENDOR MANAGEMENT POLICY

1.0 Document Control

Name	Role	Date	Version
Alfred	Infosec Manager	April	3.0

Document History

Author	Date	Version	Comment
Robin	14/04/2024	1.0	continual improvement and update to standard
Robin	15/04/2024	2.0	Transformation changed to ICT. PCER added
Robin	16/04/2024	3.0	No changes

Document Information

DOCUMENT REVIEW / APPROVAL

	NAME	DESIGNATION	SIGNATURE	DATE
Reviewed by:	Bruce Wayne	Chief Information Security Officer	Bruce Wayne	14/04/2024
Reviewed by:	Bruce Wayne	Chief Information Security Officer	Bruce Wayne	14/04/2024
Reviewed by:	Bruce Wayne	Chief Information Security Officer	Bruce Wayne	14/04/2024
Reviewed by:	Bruce Wayne	Chief Information Security Officer	Bruce Wayne	14/04/2024
Reviewed by:	Bruce Wayne	Chief Information Security Officer	Bruce Wayne	14/04/2024
Approved by:	Catwoman	Marketing Director	Catwoman	16/04/2024
Approved by:	Catwoman	Marketing Director	Catwoman	16/04/2024

2.0 Introduction

G4 Marketing Group recognizes the importance of working with reliable and trustworthy vendors to deliver successful digital marketing campaigns for our clients. This Vendor Management Policy outlines the principles and procedures for selecting, onboarding, managing, and evaluating our vendors.

3.0 Scope

This policy applies to all departments within G4 Marketing Group that engage with third-party vendors for services related to digital marketing activities, including:

- Search Engine Optimization (SEO)
- Pay-Per-Click (PPC) advertising
- Social Media Marketing
- Content Marketing
- Email Marketing
- Web Analytics
- Data Security Providers

4.0 Executive Summary

This policy ensures:

4.1 Vendor Due Diligence

We conduct thorough due diligence on potential vendors, assessing their qualifications, experience, security practices, and compliance with relevant regulations.

4.2 Contractual Agreements

We establish clear and comprehensive contractual agreements with vendors that define expectations, service levels, data security obligations, and termination clauses.

4.3 Performance Management

We monitor vendor performance regularly, track key metrics, and provide feedback to ensure they meet our requirements.

4.4 Data Security and Privacy

We select vendors with robust data security practices and ensure they comply with data protection regulations when handling client data.

By adhering to these principles, G4 Marketing Group builds strong relationships with qualified vendors, optimizes campaign performance, and manages potential risks associated with third-party involvement.

5.0 Policy

5.1 Vendor Selection

- We will establish clear criteria for selecting vendors, considering factors such as expertise, experience in relevant industries (particularly experience with regulated agencies), reputation, and cost-effectiveness.
- A formal request for proposal (RFP) process will be followed for major vendor selections, outlining project requirements and evaluation criteria.
- Shortlisted vendors will be evaluated based on their proposals, presentations, and references.

5.2 Onboarding and Contracting

- A clear onboarding process will be established to introduce new vendors to G4 Marketing Group's policies, procedures, and communication protocols.
- We will establish formal contracts with all vendors, clearly outlining the scope of services, deliverables, pricing, service level agreements (SLAs), intellectual property (IP) ownership, data security obligations, and termination clauses.

5.3 Vendor Management

- We will designate a dedicated point of contact within G4 Marketing Group for each vendor to ensure smooth communication and project management.
- Regular communication will be maintained with vendors to discuss project progress, address any issues, and provide feedback.
- Performance reviews will be conducted periodically to assess vendor effectiveness against KPIs and contractual agreements.

5.4 Data Security and Privacy

- We will only engage with vendors who implement robust data security practices to protect client information and comply with data protection regulations (e.g., GDPR, PECR).
- Vendor contracts will clearly stipulate data security requirements, including data encryption, access controls, and incident reporting procedures.

- We will conduct due diligence on vendors' data security practices and consider third-party security audits if handling sensitive client data.

5.5 Termination

- The policy will outline procedures for terminating vendor relationships in case of performance failures, breaches of contract, or security incidents.
- Clear communication will be established with vendors regarding termination procedures and potential consequences.

6.0 Prohibited Use

- Engaging with vendors who lack the necessary qualifications or experience for the required services.
- Entering into vendor contracts without proper due diligence or legal review.
- Failing to monitor vendor performance or address performance issues promptly.
- Sharing sensitive client information with vendors without contractual agreements that ensure data security.

7.0 ISO 27002:2022 Mapping

This policy aligns with the following ISO 27002:2022 domains and sub-domains:

- Domain: Asset security (A.8)
- Sub-domain: Information asset classification and labeling (A.8.2) - Classifying vendor data based on its sensitivity.
- Domain: Access control (A.9)
- Sub-domain: User access management (A.9.2) - Granting access to vendor systems only to authorized G4 Marketing Group personnel.
- Domain: Supply chain security (A.12)
- Sub-domain: Secure acquisition, use and disposal of assets (A.12.1) - Securing the selection, onboarding, and termination processes for vendors.
- Domain: Information security incident management (A.16)
- Sub-domain: Supplier relationships (A.16.4) - Including vendor communication protocols for security incidents.

8.0 Policy Compliance

All personnel within G4 Marketing Group who are involved in vendor selection, onboarding, and management are responsible for adhering to this policy. Violations may result in disciplinary action.

9.0 Regulatory Requirements

This policy considers relevant data protection regulations, such as GDPR and PECR, to ensure G4 Marketing Group meets compliance requirements when sharing client data with vendors. It also emphasizes the importance of selecting vendors who adhere to these regulations.

10.0 Marketing Context

This policy is tailored to G4 Marketing Group's marketing environment by:

- Highlighting the importance of selecting vendors with strong data security practices, especially when handling sensitive client information from regulated agencies.
- Emphasizing the need for clear contractual clauses regarding data security obligations and vendor accountability for any data breaches.
- Specifying the importance of vendor due diligence to assess their data security posture and potential risks associated with third-party involvement.

By adhering to these considerations, G4 Marketing Group demonstrates its commitment to data security and privacy throughout the vendor management lifecycle.

11.0 Policy Compliance Framework Snapshot

A comprehensive framework will be established to ensure effective policy implementation, including:

11.1 Vendor Risk Assessment

A vendor risk assessment process will be implemented to evaluate potential security risks associated with different vendors before onboarding them. This assessment will consider factors such as the vendor's data security practices, industry reputation, and experience with relevant regulations.

11.2 Vendor Contracts

Standardized vendor contracts will be developed that clearly outline:

- Service expectations and deliverables.
- Data security obligations, including encryption standards and access controls.
- Data breach notification procedures.
- Intellectual property (IP) ownership rights.
- Termination clauses for non-compliance or performance failures.

11.3 Vendor Performance Monitoring

Regular performance reviews will be conducted to assess vendor effectiveness against KPIs and contractual agreements. Metrics may include project completion rates, on-time delivery, and client satisfaction.

11.4 Vendor Communication

Clear communication channels will be established with vendors to facilitate information exchange, address performance issues promptly, and ensure alignment with project objectives.

12.0 Recommendations for Successful Implementation

12.1 Develop a Vendor Management Register

Maintain a centralized register to track all approved vendors, their contact information, service offerings, and relevant contracts.

12.2 Maintain Vendor Communication Channels

Establish clear communication channels with vendors to facilitate information exchange, project updates, and feedback.

12.3 Standardize Vendor Contracts

Develop standardized vendor contract templates that address key terms and conditions, data security obligations, and termination clauses.

12.4 Conduct Regular Vendor Reviews

Periodically review the Vendor Management Policy to ensure its effectiveness and adapt it to industry best practices and evolving regulations.