G4 MARKETING GROUP

INFORMATION CLASSIFICATION 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 protecting sensitive information entrusted to us by our clients, many of whom are regulated agencies. This Information Classification Policy establishes a standardized approach to classifying information based on its confidentiality, integrity, and availability requirements.

3.0 Scope

This policy applies to all employees, contractors, and temporary personnel working at G4 Marketing Group. It covers all information assets in physical and electronic formats, including:

- **Client data (names, addresses, contact information)**
- **Campaign materials (creative assets, marketing plans)**
- **Internal documents (financial records, employee information)**
- **Intellectual property (source code, design concepts)**

4.0 Executive Summary

This policy outlines four information classification levels: Public, Confidential, Internal, and Highly Confidential. Each classification level has specific handling and access guidelines to ensure appropriate protection. By adhering to this policy, G4 Marketing Group can maintain client trust, comply with regulatory requirements, and minimize the risk of information breaches.

5.0 Policy

5.1 Information Classification Levels:

- **Public:**

Information intended for unrestricted public disclosure (e.g., company website content, press releases).

- **Confidential:**

Information that should be protected but is not considered highly sensitive (e.g., client contact lists, internal marketing reports).

- **Internal:**

Information for internal use only and not intended for public disclosure (e.g., employee handbooks, meeting minutes).

- **Highly Confidential:**

Highly sensitive information requiring the strictest controls (e.g., client financial data, login credentials, proprietary marketing strategies).

5.2 Classification and Labeling:

- **Information will be classified based on a sensitivity assessment considering potential harm if disclosed.**
- **All information assets will be clearly labeled with their classification level.**

5.3 Access Controls:

- **Access to information will be granted based on the "need-to-know" principle.**
- **User access privileges will be reviewed and adjusted regularly.**

5.4 Security Practices:

- **Secure storage practices will be implemented for all information assets, considering format and classification level.**
- **Strong password policies and encryption will be used to protect sensitive data.**
- **Regular security awareness training will be provided to all personnel.**

6.0 Prohibited Use

6.1 Unauthorized Access:

Employees are prohibited from accessing classified information beyond their authorized clearance level, ensuring that access is limited to individuals with a legitimate need-to-know.

6.2 Unauthorized Disclosure:

Employees must not disclose classified information to unauthorized individuals or entities, protecting the confidentiality of sensitive data and proprietary information.

6.3 Unauthorized Alteration:

Employees are prohibited from altering or modifying classified information without proper authorization, preserving the integrity and reliability of data.

7.0 ISO 27002:2022 Mapping

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

- **Domain: Information security policies (A.12)**
- **Sub-domain: Information classification and labeling (A.12.6)**
- **Domain: Asset management (A.6)**
- **Sub-domain: Classification of information assets (A.6.1)**

8.0 Policy Compliance

8.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

8.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

8.3 Non-Compliance

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

9.0 Regulatory Requirements

G4 Marketing Group recognizes and complies with all relevant regulatory requirements pertaining to information security, including but not limited to GDPR, PECR, PCI DSS, and any industry-specific regulations applicable to the organization's operations, ensuring legal and regulatory compliance and minimizing potential liabilities.

10.0 Marketing Context

Considering the nature of G4 Marketing Group's operations and its clientele, adherence to this policy is critical for maintaining trust, reputation, and compliance with regulatory requirements, thereby safeguarding the organization's interests and fostering continued business growth and success.

This policy is tailored to the marketing environment of G4 Marketing Group by:

- **Considering the specific types of information handled for regulated agencies.**
- **Emphasizing the importance of client data protection and regulatory compliance.**

11.0 Policy Compliance Framework Snapshot

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

- **Awareness Training:**

Training on information classification and security procedures quarterly.

- **Policy Dissemination:**

Making the policy readily available to all personnel via intranet.

- **Regular Reviews:**

Periodically reviewing the policy and updating it as needed.

- **Incident Reporting:**

Establishing a clear channel for reporting security incidents.

12.0 Recommendations for Successful Implementation

12.1 Executive Sponsorship: Obtain visible support and sponsorship from senior management to underscore the importance of information classification and secure buy-in from all stakeholders.

12.2 Cross-functional Collaboration: Foster collaboration between IT, legal, compliance, and other relevant departments to ensure a holistic approach to information security and compliance.

12.3 Regular Review and Update: Periodically review and update the policy to reflect changes in business operations, technology, regulatory requirements, and emerging threats, ensuring its continued relevance and effectiveness in mitigating risks.