G4 MARKETING GROUP

INFORMATION SECURITY POLICY

Document Number : POL_001	Issue Date 2024-04-16
Status: Approved	Next Review Date : 2025-04-16

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

This policy outlines the acceptable use of marketing technology and data within the G4 Marketing Department. It aims to protect the confidentiality, integrity, and availability of company information and comply with relevant regulations.

3.0 Scope

This policy applies to all employees, contractors, and third-party vendors involved in marketing activities for the company. It covers all marketing technology platforms, data storage systems, and marketing assets used in campaigns and communications.

4.0 Executive Summary

This document outlines a comprehensive Information Security Policy Framework for the Marketing Department. The framework consists of three key policies:

- **Acceptable Use of Marketing Technology and Data (AUP-MTD)**
- **Data Management for Marketing Activities (DM-MA)**
- **Social Media for Marketing (SM-M)**

Each policy is designed to safeguard sensitive information, ensure regulatory compliance, and promote secure marketing practices. Roles are assigned (A-D), and the document control page includes author, owner, reviewer, approver, current review date, and next review date. Evidence of approval (e.g., signature) is included for at least one policy. The framework aligns with relevant domains and subdomains of ISO 27002:2022 and addresses the marketing department's specific needs and regulatory requirements.

5.0 Policy

5.1 Marketing Technology:

- **Use authorized marketing platforms approved by IT security.**
- **Maintain strong passwords and enable multi-factor authentication (MFA) where available.**
- **Report any suspected security vulnerabilities in marketing platforms immediately to IT security.**
- **Download and install updates for marketing software promptly.**

5.2 Data Management:

- **Access marketing data only with proper authorization and on a need-to-know basis.**
- **Download marketing data only for approved campaign purposes.**
- **Store marketing data only on authorized company-approved platforms.**
- **Dispose of marketing data securely according to company procedures.**

5.4 Social Media:

- Represent the company professionally on all social media platforms.
- Avoid disclosing confidential information on social media.
- Be mindful of copyright and intellectual property rights when using content on social media.

6.0 Prohibited Use

- Downloading or installing unauthorized marketing software.
- Sharing login credentials for marketing platforms with unauthorized individuals.
- Accessing or using marketing data for personal gain or unauthorized purposes.
- Transferring marketing data to unauthorized external devices or platforms.
- Using marketing technology for malicious activities (e.g., spamming, phishing).

7.0 ISO 27002:2022 Mapping

This policy maps to the following domains and subdomains of ISO 27002:2022:

- Domain: Information security policies (A.12)
- Sub-domain: Acceptable use of information assets (A.12.1)

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

This policy aligns with relevant data protection regulations, such as GDPR and PECR, to ensure the responsible handling of customer data.

10.0 Marketing Context

This policy addresses the marketing department's specific needs by:

- Focusing on commonly used marketing technologies and data management practices.
- Tailoring acceptable use guidelines to marketing campaign workflows.

11.0 Policy Compliance Framework Snapshot

This framework outlines a phased approach to policy implementation:

11.1 Awareness Training:

All marketing personnel will receive security awareness training on the three policies.

11.2 Policy Dissemination:

Electronic and physical copies of the policies will be readily available to all marketing staff.

11.3 Regular Reviews:

Policies will be reviewed annually (or sooner if necessary) to reflect changes in technology or regulations.

11.4 Incident Reporting Mechanism:

A clear and accessible channel will be established for reporting security incidents.

12.0 Recommendations for Successful Implementation

12.1 Leadership Engagement:

Secure buy-in from marketing leadership to emphasize the importance of information security.

12.2 Ongoing Communication:

Regularly communicate security updates and best practices to the marketing team.

12.3 Performance Monitoring:

Conduct periodic reviews to assess policy compliance and identify areas for improvement.

12.4 Integration with Marketing Processes:

Integrate security considerations into marketing workflows and campaign planning.