G4 MARKETING GROUP

IDENTITY MANAGEMENT AND ACCESS CONTROL POLICY

Document Number : POL_003	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

G4 Marketing Group recognizes the critical importance of safeguarding access to our information systems and data. This Identity Management and Access Control Policy outlines procedures for managing user identities and access privileges to ensure only authorized personnel can access the information they need to perform their job duties.

3.0 Scope

This policy applies to all employees, contractors, vendors, and any other individuals who access G4 Marketing Group's digital resources, including but not limited to computers, networks, applications, and data repositories. .

4.0 Executive Summary

This policy establishes a framework for

4.1 User Provisioning and Deprovisioning

Streamlining the process of creating and removing user accounts based on employment status and role changes.

4.2 Access Control

Granting access to systems and data based on the principle of least privilege, ensuring users only have the access they absolutely need.

4.3 Password Management

Enforcing strong password policies and promoting best practices for password hygiene.

4.4 Review and Monitoring

Regularly reviewing user access privileges and monitoring system activity for suspicious behavior.

By implementing these controls, G4 Marketing Group can minimize the risk of unauthorized access, data breaches, and insider threats.

5.0 Policy

5.1 User Provisioning and Deprovisioning:

- **User accounts will be created upon hire or contract initiation, with access privileges aligned with job responsibilities.**
- **User accounts will be disabled or deleted promptly upon termination, resignation, or project completion.**
- **Access reviews will be conducted periodically to ensure user privileges remain appropriate.**

5.2 Access Control:

- **The principle of least privilege will be strictly enforced. Users will only be granted the minimum access level required to perform their duties.**
- **Access controls will be implemented based on user roles and job functions.**
- **Access to highly sensitive information will be restricted to a limited number of authorized personnel.**

5.3 Password Management:

- **Strong password policies will be enforced, including minimum password length, complexity requirements, and regular password changes.**
- **Multi-factor authentication (MFA) will be implemented for all access points where possible.**
- **Users are prohibited from sharing passwords or using weak passwords easily guessable by others.**

5.5 Review and Monitoring:

- **User access privileges will be reviewed regularly to ensure they remain appropriate.**
- **System activity will be monitored for suspicious behavior, such as unauthorized access attempts or unusual data access patterns.**
- **Reported security incidents will be investigated promptly and appropriate action will be taken.**

6.0 Prohibited Use

- Sharing user accounts or access credentials with unauthorized individuals.
- Accessing systems or data beyond authorized permissions.
- Using weak or easily guessable passwords.
- Attempting to bypass access controls or security measures.

7.0 ISO 27002:2022 Mapping

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

- Domain: Access control (A.9)
- Sub-domain: User access management (A.9.2)
- Domain: Information security policies (A.12)
- Sub-domain: Password management (A.12.4)

8.0 Policy Compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or legal action, depending on the severity of the violation and its impact on the organization's security and compliance. .

9.0 Regulatory Requirements

This policy considers relevant data protection regulations, such as GDPR and PECR, which require organizations to implement appropriate access controls to safeguard personal data.

10.0 Marketing Context

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

- Addressing the need to protect client data entrusted to the agency by regulated agencies.
- Emphasizing the importance of access control for marketing campaigns and sensitive creative assets.

11.0 Policy Compliance Framework Snapshot

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

11.1 User Onboarding

New hires and contractors will receive training on identity management and access control procedures.

11.2 Regular Reviews

User access privileges will be reviewed periodically and adjusted as needed.

11.3 Security Awareness Training

Ongoing training will be provided to all personnel on password security and cyber threats.

11.4 Incident Reporting:

A clear channel will be established for reporting suspicious activity or potential security breaches.

12.0 Recommendations for Successful Implementation

- **Gain leadership buy-in to emphasize the importance of access control.**
- **Implement automated user provisioning and deprovisioning**