1. Purpose

This policy outlines how Corporate Communications, Inc. manages access to its digital resources. It's designed to protect client data, maintain the integrity of our systems, and ensure that only authorized personnel can access sensitive information.

2. Scope

This policy applies to all employees, contractors, and anyone else using Corporate Communications, Inc.'s digital resources, including:

- Computers and devices
- Networks (wired and wireless)
- Software and applications
- Data (client information, campaign results, financial records)
- Cloud services

3. Principles

- **Least Privilege:** Users are granted only the access necessary to perform their job duties.
- **Need to Know:** Access to specific data is restricted to those who require it for their work.
- **Separation of Duties:** Critical responsibilities are divided among multiple individuals to prevent misuse of access.
- **Regular Review:** Access rights are reviewed and updated regularly to reflect changes in job roles or security needs.

4. Roles and Access Levels

- **Account Manager:** Access to client data, project management tools, communication platforms, and campaign performance metrics.
- **Marketing Specialist (SEO, Social Media, etc.):** Access to relevant marketing platforms, analytics tools, and content management systems.
- **Creative Team:** Access to design software, asset libraries, and project-related materials.
- Development Team: Access to development and prediction environments as required
- **Administrator:** Full access to all systems for maintenance, security, and configuration.
- **Executive/Owner:** Access to high-level data, including client information, financial data, and strategic plans.
- **Intern:** Limited access to specific tools and data under supervision.

5. Access Management

- **Account Creation:** User accounts are created by the System Administrator based on job roles and manager approval.
- **Access Requests:** Requests for access beyond standard permissions must be approved by a manager and the System Administrator.

- **Passwords:**
  - Users are responsible for keeping passwords confidential.
  - Passwords must meet complexity requirements (length, character types).
  - Regular password changes are required.
  - Password sharing is prohibited.
- **Account Termination:** Access is revoked immediately upon termination of employment or contract.

6. Acceptable Use

All users must comply with the Acceptable Use Policy, which covers:

- Use of resources for business purposes only
- Protection of data from unauthorized access
- Prohibition of illegal activities
- Guidelines for using company equipment and software

7. Enforcement

Violations of this policy may result in disciplinary action, including termination of employment.

8. Policy Review

This policy will be reviewed periodically and updated as needed.

9. Contact

Questions about this policy should be directed to the Owner.

Revision History

08/26/2021

- Originated