1. Purpose

The purpose of this policy is to outline the guidelines for installing software on company-owned or company-managed devices. This policy aims to:

- Protect the agency's systems and data from security threats, including malware and viruses.
- Ensure software compatibility and prevent system instability.
- Maintain compliance with software licensing agreements.
- Optimize IT support and resource allocation.
- Safeguard client data and maintain confidentiality.

2. Scope

This policy applies to all employees, contractors, and temporary staff of Corporate Communications, Inc. who use company-owned or company-managed devices, including but not limited to laptops, desktops, mobile phones, and tablets. This policy covers all software installations, including applications, utilities, and browser extensions.

3. Policy

3.1 General Principles

- All software installations on company-owned or company-managed devices must adhere to this policy.
- Users are responsible for understanding and complying with this policy.
- The installation of unauthorized software is strictly prohibited.
- Users must not attempt to bypass or disable any software restrictions or security measures implemented by the agency.
- The agency's IT department is responsible for managing and approving software installations, ensuring compliance, and providing support.

3.2 Approved Software

- A list of approved software for specific job functions will be maintained by the IT department. This list will include software commonly used for digital marketing activities, such as:
    - Web browsers (e.g., Chrome, Firefox, Edge)
    - Office productivity suites (e.g., Microsoft 365, Google Workspace)
    - Communication and collaboration tools (e.g., Slack, Zoom)
    - Design software (e.g., Adobe Creative Cloud - with specific application approval)
    - Social media management platforms (Metricool)
    - Analytics tools (e.g., Google Analytics - access via agency accounts)
    - Project management software (HUB)
- Users are encouraged to use software from this approved list whenever possible.
- All software provided by the agency must be used in accordance with licensing agreements.
- Users are responsible for keeping their approved software up to date, or enabling automatic updates where available.

3.3 Requesting Software Installation

- If a user requires software that is not on the approved list, they must submit a formal request to the IT department.
- The request should include:
  - The name and version of the software.
  - A detailed justification for its use, including how it will support the user's job responsibilities and contribute to agency goals.
  - Any specific system requirements for the software.
  - The software's licensing terms.
- The IT department will evaluate the request based on factors such as:
  - Business need and justification
  - Security risks
  - Compatibility with existing systems
  - Licensing compliance
  - Cost
  - Support requirements
- The IT department will communicate its decision to the user in a timely manner.
- If approved, the IT department will either:
  - Install the software for the user, or
  - Provide the user with installation instructions and any necessary licenses.

3.4 Prohibited Software

- The following categories of software are strictly prohibited from being installed on company-owned or company-managed devices:
  - Software from untrusted sources or file-sharing websites.
  - Peer-to-peer (P2P) file-sharing software (e.g., BitTorrent).
  - Unauthorized games or entertainment software.
  - Software that attempts to bypass security measures.
  - Any software that violates copyright laws or licensing agreements.
  - Server software (e.g., web servers, database servers) unless explicitly required and approved for a specific job function (e.g., for a developer role)
- The IT department may maintain a list of specific prohibited software, which will be updated as needed and communicated to employees.

3.5 Software Updates and Maintenance

- The IT department is responsible for ensuring that all approved software is kept up to date with the latest security patches and updates.
- Users are expected to cooperate with the IT department in this effort, which may include:
  - Allowing the IT department to perform remote updates.
  - Restarting their devices when prompted.
  - Not disabling automatic updates for approved software.

3.6 Enforcement

- Violations of this policy may result in disciplinary action, up to and including termination of employment.
- The IT department will regularly monitor software installations on company-owned devices to ensure compliance.
- The agency reserves the right to remove any unauthorized software from company-owned devices without notice.

4. Exceptions

- Any exceptions to this policy must be approved in writing by the owner.
- Requests for exceptions should include a detailed justification and an assessment of the potential risks.

5. Review and Updates

- This policy will be reviewed and updated periodically, or as needed, to reflect changes in technology, security threats, and business requirements.
- Users will be notified of any significant changes to this policy.

By using company-owned or company-managed devices, you acknowledge that you have read, understood, and agree to comply with this User Installed Software Policy.

Revision History

04/25/2025

- Originated