Corporate Website Policy

1. Purpose
This policy governs the online representation of DevEngineers, its staff, and its partners through the organization's corporate website. It ensures a consistent, appropriate, and professional presence while fulfilling regulatory requirements and internal objectives.

2. Scope
This policy applies to all stakeholders involved in managing and publishing content on DevEngineers' web platforms, including employees, contractors, and partners who have been granted access to the Content Management System (CMS) after undergoing appropriate training. It encompasses all online content, including text, images, videos, and third-party integrations.

3. Policy

3.1 Authorized Users

Only authorized users who have completed CMS training may publish content within DevEngineers' corporate web environment. This includes employees, contractors, and partners who have been given specific roles and permissions. Unauthorized users are strictly prohibited from accessing or modifying website content.

3.2 Approval Process for Website Content

All content intended for publication must go through a formal approval process, including review for accuracy, accessibility, compliance with regulations, and alignment with DevEngineers' objectives. The approval process is as follows:

- **Step 1:** Content creation by an authorized user.
- **Step 2:** Internal review by the relevant department or team.
- **Step 3:** Final approval by the Chief Information Officer (CIO) or designated content approver.

3.3 Branding and Design Standards

All content must adhere to DevEngineers' branding guidelines, including consistency in tone, messaging, and visual design. Authorized users must use only approved CMS templates, and all media (photography, videos, etc.) must align with DevEngineers' brand image and standards.

3.4 Role of the Chief Security Officer (CSO)

The CSO, or a delegate, has the authority to review, edit, or remove content that violates this policy or misrepresents the organization. Inappropriate or non-compliant content will be flagged for immediate action.

3.5 Custom Coding and Third-Party Tools

Custom coding, third-party software, or applications are only to be used with the explicit approval of the Chief Information Officer (CIO). A thorough risk assessment must be conducted to ensure that these tools meet DevEngineers' security and functionality standards.

3.6 Content Review and Revision Process

Content on the website must be regularly reviewed to ensure accuracy, timeliness, and relevance. Quarterly reviews are mandatory for high-traffic sections of the website. Outdated or incorrect content will be updated or removed as necessary.

3.7 Online Advertising and Commercial Endorsements

DevEngineers' web pages must not feature advertising for commercial entities or third-party logos unless prior written approval has been obtained from senior management. The Brand Officer must also sign off on any external advertising content featured on the website.

3.8 Compliance with Legal and Regulatory Standards

All published content must comply with the following legal and regulatory requirements:

- **General Data Protection Regulation (GDPR)** for user privacy.
- **Web Content Accessibility Guidelines (WCAG) 2.1** to ensure content accessibility for all users, including those with disabilities.
- Other industry-specific legal frameworks as necessary.

3.9 Enforcement and Consequences for Non-Compliance

Non-compliance with this policy may result in immediate removal of the offending content by the CSO, suspension of user access to the CMS, or disciplinary action as outlined in DevEngineers' internal disciplinary procedures.

4. Record Management

The CMS administrators are responsible for maintaining a log of all content changes, approvals, and revisions. These records must be reviewed quarterly to ensure policy adherence and completeness. All versions of published content and CMS activity logs are to be archived for future reference.

5. Revision History

Date of Change	Responsible	Summary of Change	Next Review
July 2024	Chief Security Officer	Initial creation of policy	January 2025

6. Glossary of Terms

- **CMS (Content Management System):** A software application used to create, manage, and modify content on a website.
- **Branding Guidelines:** Rules that define how an organization's logo, colors, typography, and messaging are used across different platforms.
- **Authorized Users:** Employees, contractors, or partners who have completed training and have been given access to the CMS.
- **Chief Security Officer (CSO):** The person responsible for overseeing the security of online content and enforcing this policy.