AVISHA
MARKETING CO.

COMPLIANCE AND REGULATORY POLICY REPORT

AVISHEK DHAKAL
220064

Compliance and Regulatory Report

Avishek Dhakal (CU ID:12981148 | Student ID: 220064)

ST6054CEM Security Management

Ganesh Bhusal

August 17, 2024

Overview

This report outlines Avisha Marketing Co.'s comprehensive approach to managing social media compliance and risk mitigation. We analyze potential risks in areas such as data privacy, security, intellectual property rights, content moderation, user behavior, and regulatory compliance which could be a big problem for the agency. The report outlines our content creation process, emphasizing compliance and risk mitigation. We detail our monitoring, reporting, and enforcement procedures, and our training programs designed to foster a culture of compliance.

Table of Contents

Table of Figures

Figures **Page no.**

Introduction

As the Chief Compliance officer for the Digital Marketing Agency Avisha Marketing Co. that specializes in social media management, it is imperative to establish a robust Compliance and Regulatory policy. Avisha's exponential growth with diverse clients, spread across different industries has necessitated the agency for a comprehensive policy to guide the use of popular social media platforms such as Facebook, Instagram, TikTok and YouTube. Compliance of these platforms with regulatory policy is not just a legal obligation but a strategic importance. This comprehensive compliance and regulatory policy are designed to serve as a guiding framework for the agency, ensuring that our social media practices across the mentioned platform align with all the standards there too.

Purpose of the policy

The main purpose of this policy is to mitigate the risks associated with social media engagement while safeguarding the clients' interests and agency's reputation. By adhering to this policy, we aim to:

i. Mitigate Legal Risk: Ensure Compliance with different regulations, including data protection laws, advertising standards and platform-specific rules.
ii. Protect User Data: Implement robust security practices to safeguard user data from unauthorized access, breaches and misuses.
iii. Uphold Ethical Standards: Promote transparency, honesty and fairness in all social media interactions.
iv. Preserve Brand Reputations: Avoiding any sort of negative publicity and potential legal actions that could arise from non-compliant practices.

Scope of the Policy

It encompasses all aspects of social media management, from content creation and publication to data handling and advertising practices.

Importance of Policy Compliance

The increasing use of social media platforms has allowed businesses to shift from traditional forms of marketing and advertising to new and improved digital marketing. So, as an agency, it is crucial for us to avoid anything that would put us negatively in the market. So, it is necessary to follow this policy as this may lead to scenarios including:

i. Legal Penalties: Huge fines and legal cases for violating data protection laws or engaging in deceptive advertising.
ii. Reputational Damage: People losing trust from Avisha leading to decreased business opportunities.

Objectives of the policy

1. To ensure our agency's social media management practices align with the best industry practices and comply with all relevant regulatory standards.
2. To mitigate potential legal and reputational risks associated with the misuse of social media.
3. To establish clear guidelines for content creation, publication, moderation, data privacy, and security on each social media platform.
4. To establish a culture of compliance within our organization through regular training and awareness programs.

Overview of Frameworks and Guidelines

Compliance with social media requires a structured approach guided by established frameworks and regulations. This section provides an overview of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and other applicable guidelines, highlighting their relevance of effective social media engagement.

NIST Framework Overview

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a voluntary set of standards to help organizations manage and reduce cybersecurity risks. While not specific to social media, its core functions provide a valuable roadmap for ensuring secure and compliant social media practices:

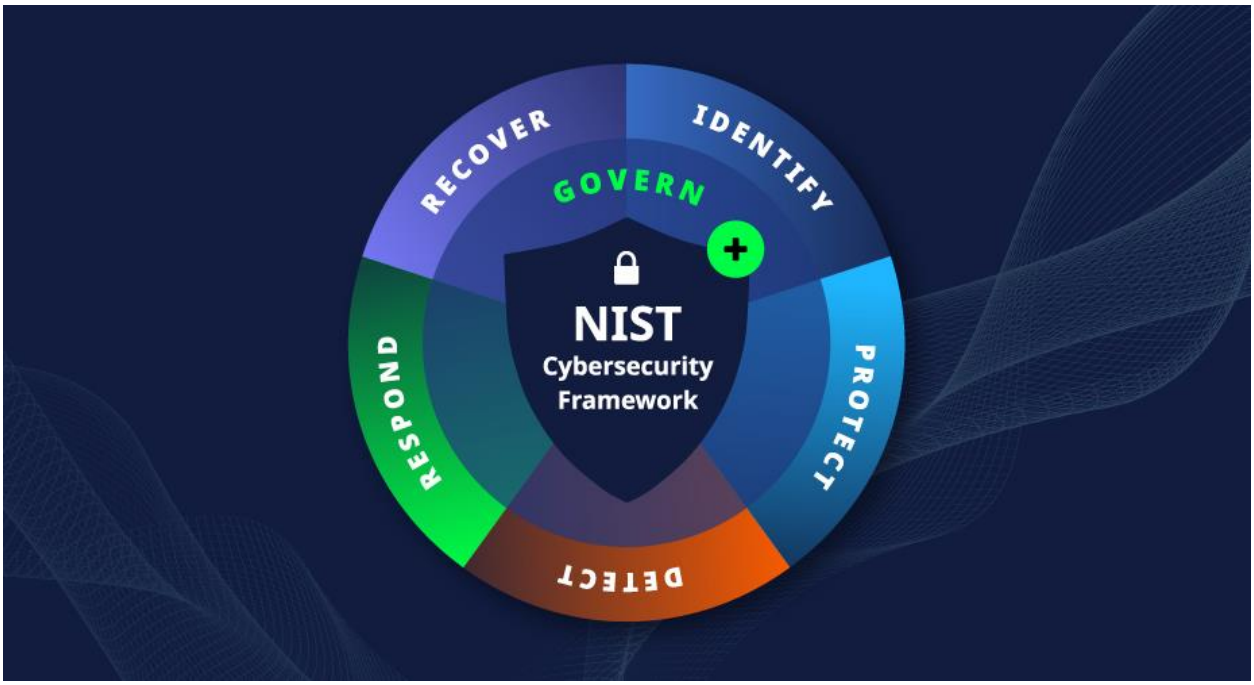

Figure 1: NIST framework

1. Identity

   This helps organizations understand cybersecurity risks to system, data and capabilities. In the context of social media, it involves identifying potential vulnerabilities and risks associated with each platform such as data, breaches, unauthorized access and misinformation.

2. Protect

   It guides the organization with appropriate safeguards to ensure the delivery of critical services. Whereas in case of social media compliance this may include things like creating incident response plans for various scenarios such as account compromise of data leaks.

3. Detect

   The function involves developing and implementing activities to identify cybersecurity events. In social media management, this translates to monitoring social media accounts for suspicious activity, such as unauthorized posts, unusual logins or privacy violations.

4. Respond

   It focuses on acting regarding detected cybersecurity events. For social media, this may involve creating incident response plans for various scenarios, such as account compromise or data leaks.

5. Recover

   The last function primarily focuses on maintaining plans for resilience and restoring capabilities impaired by cybersecurity incidents. In the social media context, this includes strategies for reputation management and service restoration after a security incident.

Relevant Guidelines

In addition to NIST framework there are other several other guidelines that significantly affect social media compliance.

General Data Protection Regulation (GDPR)

The GDPR is a comprehensive data protection law that applies to all organizations operational in the European Union (EU) and processes the personal data of people residing there *(General Data Protection Regulation (GDPR) –, 2024).* For our agency GDPR compliance is crucial as we manage many clients from Europe.

Key principles of GDPR relevant to social media management:

i. Lawful, fairness and transparency: All data processing on social media platforms must be lawful, fair, and transparent to users.
ii. Purpose limitation: Personal Data collected through social media should only be used for explicitly specificized legitimate purposes.
iii. Data minimization: Only collect and process data that is necessary for specific purpose of your social media campaigns.
iv. Accuracy: Ensure that the personal data stored and used for social media marketing is accurate and kept up to date.
v. Storage limitation: Retain personal data only for as long as necessary for marketing only.
vi. Integrity and Confidentiality: Implement appropriate security measure to protect personal data collected through social media platforms.
vii. Accountability: Be able to demonstrate compliance with GDPR principles in all social media activities.

California Consumer Privacy Act (CCPA)

Like GDPR was focused for the EU citizens similarly California Consumer Privacy Act (CCPA) is state-specific law that focuses on consumer protection and privacy rights for residents of California *(California Consumer Privacy Act (CCPA), 2018)*. While like GDPR in few aspects, it has unique features relevant to social media compliance like focusing on consumer rights regarding personal information, gives consumers the right to opt-out of the sale of their personal information and required businesses to disclose data collection and sharing practices. For Avisha CCPA compliance means:

i. Updating privacy policies to reflect CCPA requirements.
ii. Implementing mechanisms for California residents to exercise their rights.
iii. Ensuring transparency in data collection and sharing practices.
iv. Providing the options to opt-out of data sales to the users.

COPPA (Children's Online Privacy Protection Act)

The Children's Online Privacy Protection Act (COPPA) is particularly relevant for social media platforms that may attract users under 13 years old (*Children's Online Privacy Protection Rule ("COPPA"), 2013)*. The law requires parental consent for collecting personal information from children under 13, mandates clear privacy policies and emphasizes the protection of children's personal information. So, the agency should pay extra attention to these and make sure the existing policy is COPPA compliant.

Comparative Table of Frameworks and Guidelines

ASPECT	NIST	GDRP	CCPA	COPPA
FOCUS	Cybersecurity	Data Protection	Consumer Privacy	Children's Privacy
SCOPE	Global	EU/EEA	California	US(Children)
KEY ELEMENTS	5 core fucntion	7 principles	4 rights	Parental consent
RELEVANCE TO SOCIAL MEDIA	High	High	High	High for youth-oriented platforms

Figure 2: Comparative table of frameworks discussed.

Introduction to Threat Modeling and Risk Assessment for social media

When talking about Risk analysis/assessment for anything the first approach is always to model threat associated with it and for that threat modelling is condicted. Threat modelling is structured approach for identifying and addresing potential security risks in an organizations's sytem and process. For Avisha threat modelling is important for protecting clients data and ensuring regulatory compliance.

Threat Modeling Methodology

For our threat modeling process, we employ the STRIDE methodology, widely recognized in the cybersecurity industry. STRIDE is an acronym representing six categories of threats (for, 2023) :

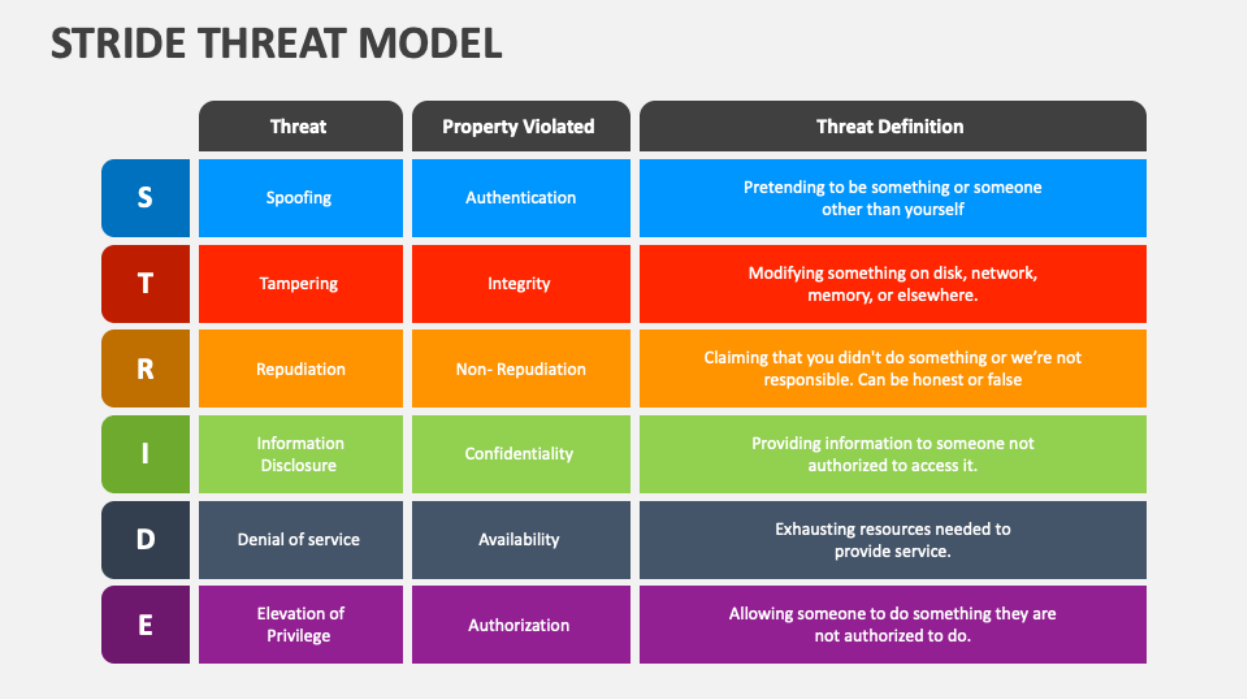

Figure 3: STRIDE Threat Modeling

The diagram below shows our key assets of our social media management operation.

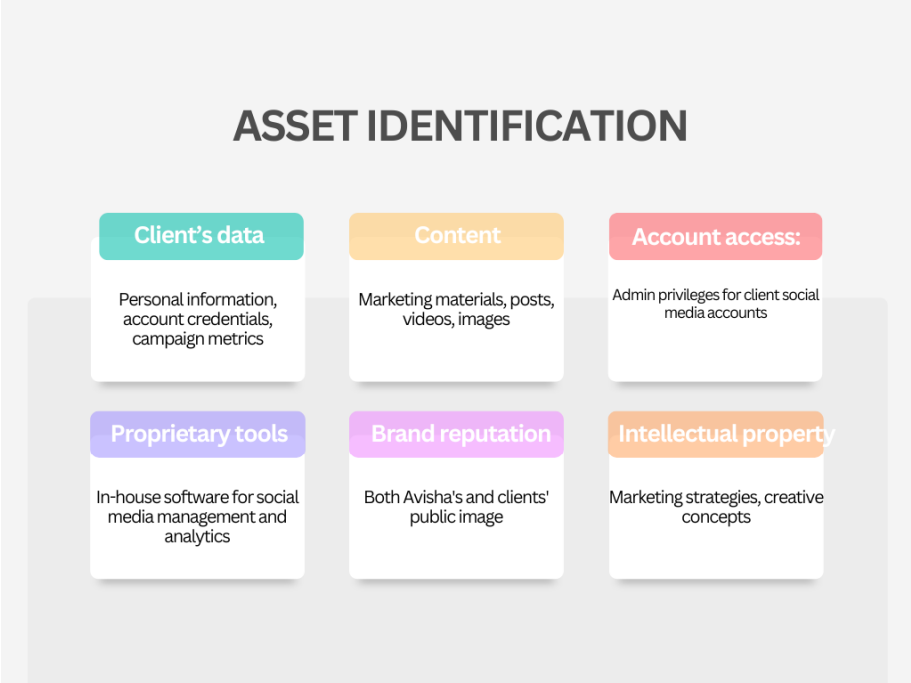

Figure 4: Assets of Avisha

Data Flow Diagram

A simplified data flow for Avisha's social media management process:

Clients ←→Avisha Marketing co. ←→ Social Media Platforms←→Third Party Tools Services

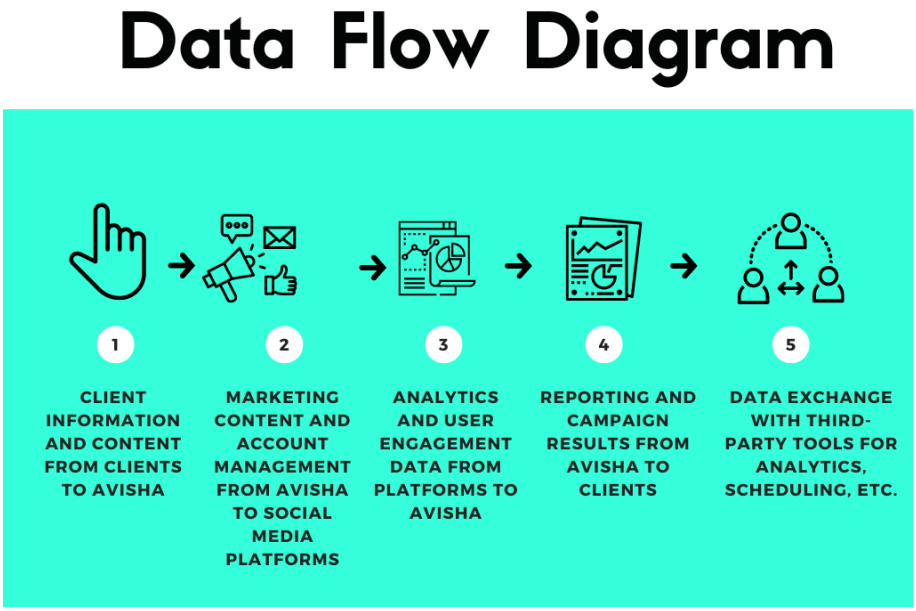

Figure 5: Data Flow Diagram

Threat Identification and Analysis

Using the STRIDE methodology, we identify and analyze the following key threats for Avisha Marketing Co.'s social media management operations:

- Spoofing: Unauthorized access to client accounts through credential theft
- Tampering: Malicious modification of client content or campaign data
- Repudiation: Denial of actions taken on behalf of clients
- Information Disclosure: Unauthorized exposure of client or user data

- Denial of Service: Disruption of social media management services
- Elevation of Privilege: Unauthorized escalation of access rights

Analysis reveals that Information Disclosure and Spoofing pose the highest risks due to their potential impact on client trust and data privacy. Elevation of Privilege and Tampering present moderate risks, while Denial of Service and Repudiation are assessed as lower risks due to existing platform protections and logging mechanisms.

So, after the threats have been identified we now move towards risk assessment of the threats we uncovered in detail. This risk assessment will focus on four major social media platforms: Facebook, TikTok, Instagram and YouTube as these are mostly used by our clients. By conducting a thorough risk assessment, we can develop targeted strategies to enhance compliance efforts and safeguard our operation.

Common Risks Across Platforms

a. Data Privacy ans Security Risks:
    I. Unauthorized access to clients social media accounts.
    II. Data breaches daily which exposed our clients or user information.
    III. The sensitive user data collected are not propelry handled by these big platforms.
b. Content-Related Risks:
    I. Accidental publication of unapproved or sensitive content
    II. Copyright infringement in posted content (e.g., using unlicensed images or music)
    III. Posting content that violates platform-specific guidelines
c. Compliance-Related Risks:
    I. Violations of data protection regulations (e.g., GDPR, CCPA)
    II. Non-compliance with advertising standards or disclosure requirements

III. Failure to adhere to age-specific regulations (e.g., COPPA)

d. Reputational Risks:

I. Negative publicity due to inappropriate content or responses

II. Brand damage from association with controversial topics or users

III. Loss of client trust due to mismanagement of their social media presence

e. Operation Risks

I. Service disruptions due to platform changes or API issues

II. Employee misuse of client social media accounts

III. Ineffective crisis management during social media emergencies

f. Financial Risks

I. Monetary losses due to regulatory fines or penalties

II. Loss of clients due to compliance failures or reputational damage

III. Unexpected costs related to security incidents or data breaches

These identified risks are directly related to Avisha Marketing Co.'s social media management activities and align with the threats we uncovered during our threat modeling exercise

Overall Risk Evaluation

It is obvious to conclude that all the discussed platforms certainly pose some risks which can be factored onto various levels. There are various risks we discussed that can be mitigated by our efforts while some are there which we cannot mitigate with just our own effort. Below is a table that summarizes our risk analysis for different platforms with respect to risks we have discussed.

Overall Risk Analysis

RISK CATEGORY	LIKELIHOOD	IMPACT	OVERALL RISK LEVEL
DATA PRIVACY AND SECURITY	High	High	High
CONTENT-RELATED	Medium	High	High
COMPLIANCE	Medium	HIgh	High
REPUTATIONAL	Medium	High	High
OPERATIONAL	Low	Medium	Medium
FINANCIAL	Low	High	Medium

Figure 6 : Risk analysis Table

Risk Mitigation Strategies

While all the risked we discussed about these platforms may not be under our control but some sure are and there are a few things that we can properly follow to mitigate the risks. We need to put in our best effort for the risk we can mitigate from our side. The figure below summarizes the necessary steps that can be taken:

Figure 7: Risk Mitigation Strategies

Data privacy and Security Measures

Avisha is entrusted with vast amount of client's sensitive information of these discussed social media platforms. It is our duty to handle the client's information properly, as the consequences for mishandling the data can be severe for the agency and clients.

The first step in handling and collecting user data is to take all the necessary consent required for us to be able to work with that data. At Avisha, we have developed a comprehensive approach for obtaining and handling user consent that aligns with key regulations like GDPR and COPPA. Here's how we implement this for our clients:

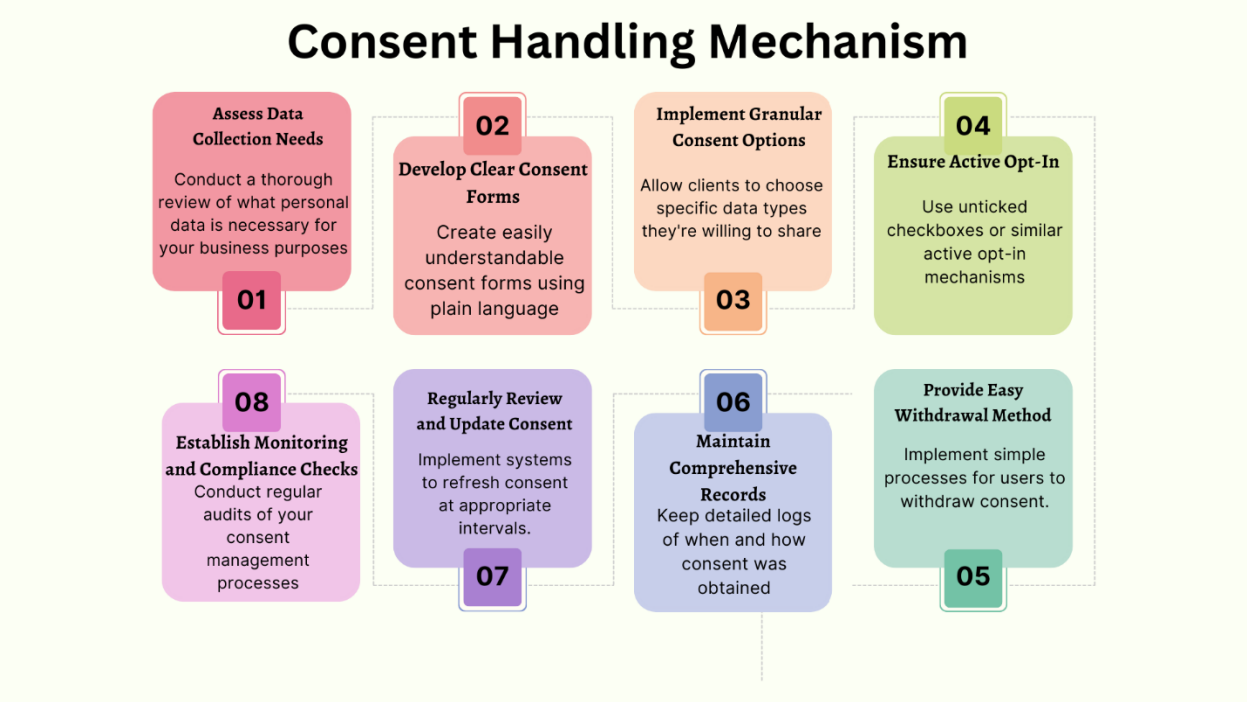

Figure 8: Consent handling Mechanism at Avisha

The above is the 8-step mechanism developed here at the agency for handling user consent. Let's dive into how Avisa put the mechanism it has developed into practice. Say we are working with "GreenLeaf Organics" a small organic skincare company looking to boost their social media presence. Here's how we would approach it.

1. **Initial Data Assessment**: We sit down with the company executives to figure out what we need. For this company, we decided we need:
    - Customer demographics (age range and location)
    - Purchase history (types of products bought)
    - Email engagement rates
    - Social media interaction data

2. **Consent Acquisition**: We then present the consent form, which is clear, straightforward document which might say something like:

"Avisha will collect and use the following data for GreenLeaf Organics' social media campaigns:

- Customer age ranges and locations
- Types of products purchased.
- Email open and click rates.
- Social media likes, comments, and shares

We'll use this data to target ads, create engaging content, and measure campaign success. We'll store this data securely and won't share it with third parties without your explicit permission."

3**. Regulatory Compliance**: We explain to company executives that our processes comply with GDPR and COPPA. For example, we say that: "We'll only keep this data for the duration of our contract plus 3 months for analysis purposes. You can request to see, modify, or delete this data at any time. If we have a data breach, we'll notify you within 72 hours (about 3 days).

This is how the mechanism we have introduced is put Infront of client in the process of data collection with consent while complying relevant laws.

Secure data storage and transmissions

After the consent is properly acquired, our next utmost priority here at Avisha is client's information security privacy and information security. This is something we take very seriously. The data collected from the clients we need to use should be transmitted and stored properly. The data is Rest and Transit both are properly secured.

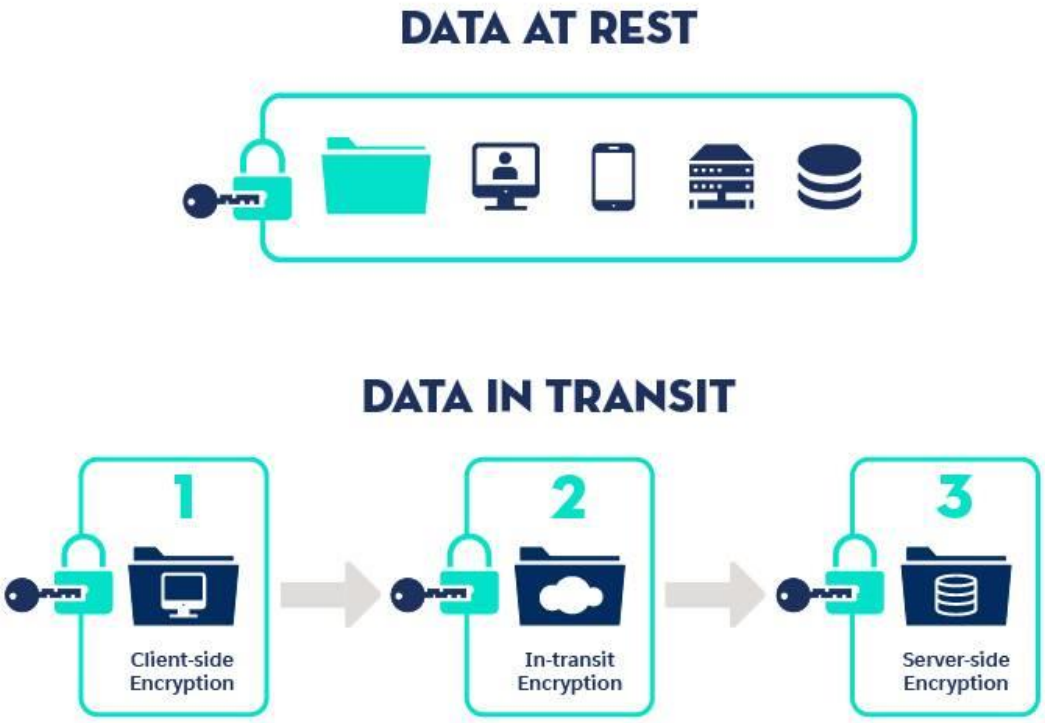

Figure 9: Data at rest and transit

1. **Data Storage Practices**

   At Avisha, we take Greenleaf Organics' data security seriously. We store their customer information in a secure cloud environment with strict access controls. For instance,

GreenLeaf's customer purchase history is classified as sensitive and is stored separately from general marketing data. Only authorized team members can access this information using multi-factor authentication. We also maintain regular backups of GreenLeaf's data, ensuring quick recovery in case of any unforeseen events.

2. **Encryption Methods**

   We employ robust encryption for GreenLeaf's data both at rest and in transit. Their customer database is encrypted using industry-standard AES-256 encryption when stored. When GreenLeaf's team accesses their campaign analytics dashboard, all data is transmitted using TLS 1.3 protocol, ensuring end-to-end encryption. This means that even if someone intercepted the data during transmission, they couldn't decipher it without the encryption keys, which are securely managed and regularly rotated.

3. **Data Transmission**

   When we need to transfer large datasets, like GreenLeaf's quarterly sales reports, we use secure file transfer protocols (SFTP). For day-to-day communications about campaign strategies or customer insights, we use a secure messaging platform with end-to-end encryption. Additionally, when GreenLeaf's team accesses our systems remotely, they do so through a VPN, adding an extra layer of security. We also have systems in place to monitor and log all data transfers, allowing us to quickly detect and respond to any unusual activity.

Content Management and Compliance

The agency will be creating a lot of content based on the client's requirements and need to improve their social media presence. There is nothing wrong with publishing good content, but they should not be targeted, harmful, stolen or deceptive. Here at Avisa proper guidelines is established to avoid any sort of such problem and make sure it is in compliance with copyright, trademark, and other intellectual property laws.

Copyright Compliance Guidelines

I. Conduct thorough checks for copyrighted material before using any content in social media posts.
II. Proper License or permission should be obtained for all third-party content, including images, music and video clips.
III. Implement a system to track and document all content licenses and permissions.
IV. Train staff on fair use principles and how they apply to social media content creation.
V. Develop clear guidelines for attributing sources when sharing or repurposing content.

Trademark Compliance Guidelines

I. Maintain an updated database of client trademarks and those of key competitors.
II. Implement a review process to ensure trademarks are not used in a way that could be considered disparaging or diluting.
III. Create guidelines for using hashtags that include trademarks, ensuring they don't imply false endorsement or affiliation.
IV. Develop procedures for addressing trademark infringement by third parties on client social media accounts.

Content Creation and review process

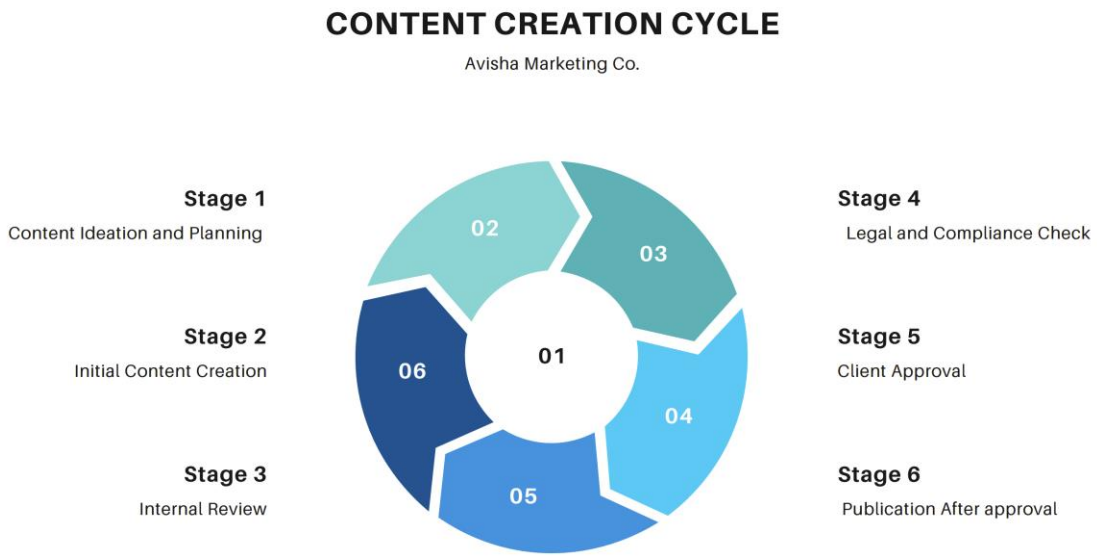

Figure 10: Content Creation Cycle

At Avisha Marketing Co., we have implemented a comprehensive six-step content creation and review process to ensure compliance and mitigate risks across all social media platforms. The cycle begins with Content Ideation and Planning, where we brainstorm ideas aligned with client goals and consult our Intellectual Property database. This is followed by Initial Content Creation, where we develop original content or use properly licensed materials. The third step involves an Internal Review to check for brand consistency and potential IP issues. Next, we conduct a Legal and Compliance Check to ensure adherence to copyright laws and platform-specific guidelines. The fifth step is Client Approval, where we present the content along with a compliance summary. Finally, we move to Publication, where we schedule and publish the approved content, maintaining thorough records for future reference. This cyclical process ensures that all content

we produce and publish is not only engaging but also compliant with relevant laws and regulations.

Monitoring, Reporting, and Compliance Enforcement

The content creation and compliance needs a proper procedure and guidelines to help monitor activities and in any case of compliance breaches help us notify.

Procedures for Monitoring Social Media Activities

We implement a comprehensive monitoring system to detect compliance breaches across all social media platforms. This includes:

- **Automated scanning**: We use advanced tools to continuously scan for potential IP infringements, unauthorized use of trademarks, and deceptive advertising practices.
- **Regular content reviews**: Our team conducts periodic reviews of all published content, including influencer posts, to ensure ongoing compliance with FTC guidelines and proper disclosures.
- **Employee activity monitoring**: We maintain oversight of employee social media activities to prevent inadvertent disclosure of sensitive information or policy breaches.

Protocols for Reporting Violations and Handling Compliance Incidents

To ensure prompt and effective handling of compliance issues, we have established the following protocols:

- **Compliance reporting system**: We've implemented a dedicated hotline and online portal for anonymous reporting of potential violations.

- **Incident investigation procedure**: A step-by-step process guides our team through investigating reported incidents, including documentation requirements and response timelines.
- **Compliance committee**: A designated committee reviews serious incidents and determines appropriate actions based on the severity and context of the violation.

Disciplinary Actions and Penalties for Non-Compliance

We enforce compliance through a tiered system of disciplinary actions:

- **Minor violations**: First-time offenses typically result in additional training or written warnings to prevent recurrence.
- **Repeated or serious violations**: These may lead to suspension of social media privileges or other job-related consequences, depending on the nature of the breach.
- **Severe breaches**: Violations that result in significant legal or reputational risks for the company may lead to termination of employment.

By implementing these robust monitoring, reporting, and enforcement procedures, we maintain a strong culture of compliance throughout our social media activities. This approach aligns with our content creation process and helps protect both our clients' interests and our company's reputation in the digital space.

Training and Awareness Programs

At Avisa, we recognize that a well-informed team is crucial for maintaining compliance in our social media activities. Our training and awareness programs are designed to educate employees about compliance policies and procedures while fostering a culture of compliance throughout the organization.

Comprehensive Training Programs

We have developed a robust training curriculum that covers all aspects of social media compliance:

- **Onboarding Compliance Training**: New employees undergo an intensive compliance orientation, covering our social media policies, IP laws, and advertising standards.
- **Regular Refresher Courses**: All team members participate in quarterly refresher sessions to stay updated on the latest compliance requirements and best practices.
- **Specialized Modules**: We offer targeted training on specific topics such as:
    - Intellectual Property Rights in Digital Content
    - FTC Guidelines for Influencer Marketing
    - Truth in Advertising on Social Media Platforms

Our training is delivered through a combination of in-person workshops, interactive online modules, and case study discussions. This multi-faceted approach ensures that employees can apply compliance principles in real-world scenarios.

Fostering a Culture of Compliance

We believe that compliance should be ingrained in our organizational culture, not just a set of rules to follow. To achieve this:

- **Leadership Commitment**: Our senior management regularly communicates the importance of compliance and leads by example in adhering to all policies.
- **Compliance Champions**: We've established a network of "Compliance Champions" across departments who promote best practices and serve as resources for their colleagues.
- **Integration into Daily Operations**: Compliance considerations are built into our content creation workflow, as outlined in our earlier processes, making it a natural part of every project.
- **Open Communication**: We encourage employees to ask questions and raise concerns about compliance issues without fear of reprisal, fostering a transparent and ethical work environment.
- **Recognition Programs**: Employees who demonstrate exceptional commitment to compliance are recognized and rewarded, reinforcing the value we place on ethical behavior.

References

- NIST. (2016, November 30). *NIST Risk Management Framework*. NIST. https://csrc.nist.gov/projects/risk-management/about-rmf
- Foo Yun Chee. (2024, May 16). *Meta faces EU investigation over child safety risks*. Reuters. https://www.reuters.com/technology/meta-faces-eu-investigation-over-child-safety-risks-2024-05-16/
- *Policy*. (2022, March 3). Federal Trade Commission. https://www.ftc.gov/policy
- Tague, A. (2020, March 3). *Ultimate Guide to Content Creation: Outlining the Process in Four Key Phases [eBook]*. ClearVoice. https://www.clearvoice.com/resources/content-creation-process/
- *About compliance, monitoring and enforcement*. (2021, February). Ministry for the Environment; Ministry for the Environment. https://environment.govt.nz/publications/compliance-monitoring-and-enforcement/about-compliance-monitoring-and-enforcement/
- for, D. (2023, May 16). *Conducting a STRIDE-based threat analysis*. GOV.UK; GOV.UK. https://www.gov.uk/government/publications/secure-connected-places-playbook-documents/conducting-a-stride-based-threat-analysis
- *General Data Protection Regulation (GDPR) – Final text neatly arranged*. (2024, April 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/
- *Children's Online Privacy Protection Rule ("COPPA")*. (2013, July 25). Federal Trade Commission. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
- *California Consumer Privacy Act (CCPA)*. (2018, October 15). State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa