We at Bang Albino are committed to ensuring an optimal IT Security environment, which involves an unwavering adherence to the following critical areas:

Security Commitments

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Up time availability of production systems

Confidentiality Commitments

- The use of encryption technologies to protect system data both at rest and in transit
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties
- Confidential information must be used only for the purposes explicitly stated in agreements between Bang Albino and client entities

Penetration Testing

Bang Albino engages with a top-tier penetration testing consulting firm in the industry on an annual basis, reaping numerous benefits, such as:

- Identifying vulnerabilities in digital infrastructure, ensuring that sensitive client data and marketing assets remain secure.
- Reducing the risk of data breaches and potential damage to Bang Albino's reputation, by proactively identifying and addressing security weaknesses.
- Meeting regulatory requirements, such as GDPR or HIPAA, ensuring Bang Albino remains in compliance with data protection laws.
- Establishing a secure digital environment, which allows our team to focus on marketing strategies and campaigns without the distractions and downtime caused by security incidents.
- Creating effective incident response plans, ensuring a swift and efficient reaction to any security breach.
- Providing peace of mind, knowing that Bang Albino's digital assets and client data are well-protected against cyber threats.

Enterprise Security:

1. **Endpoint Security**

Our corporate devices are under centralized management and come equipped with mobile device management software and anti-malware protection. We maintain continuous 24/7/365 monitoring for endpoint security alerts. To ensure secure endpoint configurations, we rely on Microsoft Intune software, which enforces practices like disk encryption, screen lock settings, and software updates.

2. **Security Awareness Training**

At Bang Albino, we deliver thorough security education to our staff during their onboarding process and on an annual basis, utilizing educational modules within the Curricula platform. Additionally, all new employees are required to participate in mandatory live onboarding sessions that emphasize fundamental security principles and secure coding practices.

3. **Identity and Access Control**

At Bang Albino, our employees' access to applications is determined by their roles and is automatically revoked when their employment ends. Additional access is granted based on the specific application's policies and requires approval accordingly.

Vendor Security Assessment

Bang Albino employs a risk-oriented method for evaluating vendor security. Various factors that impact a vendor's inherent risk assessment encompass:

- Accessibility to customer and corporate data
- Integration with production systems
- Potential impact on the Vanta brand

Once the initial risk assessment is established, we proceed to assess the vendor's security to ascertain a residual risk assessment and make an informed decision regarding vendor approval.