VioPixel Cybersecurity Policy
Effective Date: 03/01/2019

1. Purpose

At VioPixel, we prioritize security as an essential part of our commitment to **Creativity First** and **Transparency is Key**. This Cybersecurity Policy establishes guidelines to protect VioPixel's digital assets, client data, and internal systems from cyber threats while ensuring seamless and secure collaboration.

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who access VioPixel's networks, systems, or data. It covers:

- Company-owned and personal devices used for work
- Internal and client data stored or transmitted through VioPixel's systems
- Communication channels, software, and cloud-based platforms

3. Security Responsibilities

3.1 Employee Responsibilities

All employees and contractors must:

- Use strong, unique passwords and enable multi-factor authentication (MFA) where applicable.
- Store sensitive files in approved, encrypted storage solutions.
- Lock devices when not in use and report lost or stolen devices immediately.
- Refrain from downloading unauthorized software or using unapproved cloud storage services.
- Complete mandatory cybersecurity training and report suspicious activity.

3.2 IT & Security Team Responsibilities

VioPixel's IT team is responsible for:

- Implementing firewalls, antivirus software, and intrusion detection systems.
- Regularly updating and patching systems to prevent vulnerabilities.
- Conducting security audits and risk assessments.
- Monitoring network activity and responding to potential security incidents.

4. Data Protection & Encryption

- All confidential and sensitive data must be encrypted during storage and transmission.
- Employees must use company-approved VPNs when accessing systems remotely.
- Sensitive information must only be shared through encrypted communication channels.

5. Acceptable Use of Technology

- Employees may only use company-approved devices and networks for work purposes.
- Personal devices used for work must meet security standards and be registered with IT.
- Public Wi-Fi must be avoided unless using a secure VPN.

6. Phishing & Threat Awareness

- Employees must be cautious of suspicious emails, links, and attachments.
- No employee should share login credentials, even with internal personnel.
- Any suspected phishing attempts or security breaches must be reported immediately.

7. Incident Response & Reporting

In the event of a cybersecurity incident:

- Employees must report breaches to the IT team immediately.
- The IT team will assess the impact, contain the threat, and implement recovery measures.
- Affected parties will be notified in compliance with legal and contractual obligations.

8. Enforcement & Consequences

Failure to comply with this policy may result in disciplinary action, up to and including termination. Legal action may be pursued in cases of gross negligence or malicious intent.

9. Continuous Improvement & Compliance

Cybersecurity is an ongoing effort at VioPixel. We conduct regular security training, updates, and audits to stay ahead of emerging threats. Compliance with industry regulations and best practices ensures that we protect our clients, employees, and business.