36 Long Alley

Saratoga Springs, NY 12866

(518) 583-0639

Information Security Cyber Risk Third-Party Service Provider Vendor Information

Creative Compliance has established a comprehensive program framework that has an organizational structure for information security with appropriate resources, controls, conducts information risk assessments, ongoing situational awareness, threat and vulnerability risk management, security incident management, and governance.

1. OVERVIEW

Creative Compliance Software Solutions, LLC hereinafter referred to as "CREATIVE COMPLIANCE", “COMPANY” or “FIRM” recognize the importance of protecting customer sensitive electronic data to minimize the risk that such data may be exploited.

Included in this document are the most common requested cyber security polices and procedure information for Creative Compliance. This information summarizes the standards and procedures utilized by Creative Compliance.

A. Cybersecurity Definition

Cybersecurity is defined to mean actions taken to protect against the unauthorized use of customer sensitive electronic data through use of policies, encryption software, firewalls and passwords. Cybersecurity protects against the unauthorized use of customer sensitive data stored in Creative Compliance’s electronic information resources (aka, “information systems”), including but not limited to, interconnected systems or subsystems and equipment used in the storage, management, control, reception and transmission of data including hardware and software and data stored in electronic information resources, telecommunications and/or computer-related equipment, copiers, printers, mobile devices and related equipment.

2. CYBERSECURITY OVERSIGHT AND CONTROLS

A. Information Custodian

Creative Compliance deploys the company’s Chief Technology Officer (CTO) as firm’s Information Custodian and Information Security Officer. The CTO or his assign are responsible for maintaining and protecting information security including preventing attacks of data through use of information systems.

C. **Cybersecurity Committee**
Creative Compliance deploys a Cybersecurity Committee made up of Creative Compliance's most senior persons including its Principals, CTO, Corporate Compliance Manager, and Marketing Director that is responsible for cybersecurity policy review and long-term cybersecurity mapping.

D. **SOC 2 Compliance**
Developed by the American Institute of CPAs (AICPA), SOC 2 defines criteria for managing customer data based on five "trust service principles" - security, availability, processing integrity, confidentiality and privacy. Creative Compliance undergoes regular reviews and annual audits to ensure the requirements of each of the five trust principles are met and that we remain SOC 2-compliant.

E. **New York State 23 NYCRR 500**
The New York State Department of Financial Services (NYSDFS) published Cybersecurity Regulations in 2017 (23 NYCRR 500) which requires all licensed entities to establish and maintain cybersecurity programs to protect their systems and data as well as conduct due diligence into the risks presented by its third-party service providers. Creative Compliance undergoes regular reviews to ensure we meet or exceed the requirements of the NYSDFS cybersecurity regulation as a third-party service provider.

F. **Security Risk Assessments**
Audits of Creative Compliance procedures, owned equipment and physical location is performed annually to ensure that protected data is stored in approved information systems and locations. The purpose of this is to ensure compliance with this policy and to continuously improve Creative Compliance cybersecurity business practices.

G. **Cyber Security Insurance**
Creative Compliance purchases and maintains insurance covering losses for information security and privacy liability arising out of the company's acts or omissions.

3. CYBERSECURITY STANDARDS EXECUTIVE SUMMARY

A. **Written Information Security Program**
Creative Compliance has a written information security program, based on compliance with a standardized framework, which addresses how the Creative Compliance identifies and manages its cybersecurity risks and protects non-public information.

B. **Periodic Risk Assessments**
Creative Compliance internally or using a third-party conducts periodic risk assessments to identify risks in relation to non-public information and information systems.

C. **Records Retention Policy**
Creative Compliance has a records retention policy that requires the destruction of non-public information when it is no longer needed to fulfill a business obligation or legal requirement.

D. **Third Party Compliance Reviews**
Creative Compliance has a process in place to review the cyber security risks associated with its third-party vendors and requires its vendors to notify Creative Compliance in the event of a breach.

E. **Employee Security Training**
Creative Compliance requires all employees with access to non-public information to attend security awareness training.

F. **Administrative Controls**
Creative Compliance uses administrative controls to manage user identification and access, including, minimum password length and complexity, frequent password changes, user lockout after unsuccessful login attempts, and multi-factor authentication.

G. **Technical Controls**
Creative Compliance uses technical controls to safeguard non-public information, including firewalls, updated anti-virus software and encryption of data on laptops and mobile devices

H. **Access Controls**
Creative Compliance restricts access to non-public information to only those users for whom access is required to fulfil their job responsibilities.

I. **Data Encryption**
All non-public information is stored for best practices of data at rest and in transit.

4. SECURITY CONTROLS AND PROCEDURES

A. Information Security Overview
Creative Compliance's practice is to protect against unauthorized access use, disclosure, disruption, modification, or destruction of Creative Compliance information systems through implemented policies, procedures, and controls to protect data including technical measures to detect, respond and mitigate damage from a cyberattack. Controls include data encryption; malware defenses including anti-virus, anti-spyware, and host-based IDS features; security software management including software network management; email and web browser protection utilizing spam-filtering tools and blocking malicious web domains. Additional controls include managing the security configuration of network infrastructure devices (firewalls, routers and switches); inventory and control of hardware assets; managing operational use of ports, protocols and services on managed network devices; managing the security configuration of servers, workstations and portable devices; control and management of application and system lifecycles to prevent systems and accounts from being leveraged; controlled use of administrative privileges on computers, applications and the network; wireless access controls; maintenance, monitoring and analysis of audit logs; and incident response and management.

B. Data Security
All non-public information stored in Creative Compliance owned Information Systems is stored for best practices of data at rest and in transit.

C. Physical Security
Creative Compliance owned Information Systems are physically secured. Access to IT equipment is restricted to only those whose responsibilities require they maintain the equipment or infrastructure primarily the CTO or his assigns. Dedicated space is committed to company server(s) and IT equipment and camera monitored. Physical documents containing Class IV data are shredded, and other documents securely disposed of along with unwanted Information system components.

D. Network Security

Creative Compliance uses technical controls to safeguard non-public information, controls include managing the security configuration of network infrastructure devices (firewalls routers and switches); inventory and control of hardware assets; managing operational use of ports, protocols and services on managed network devices; managing the security configuration of servers, workstations and portable devices (laptops, tablets, smart phones); control and management of application and system lifecycles to prevent systems and accounts from being leveraged; controlled use of administrative privileges on computers, applications and the network; wireless access controls; maintenance, monitoring and analysis of audit logs.

E. Network Segmentation

Creative Compliance's network infrastructure is segmented across geographic locations, business units and webservices.

F. **Employee Security**

Creative Compliance utilizes administrative controls to manage user identification and access, including, minimum password length and complexity, frequent password changes, user lockout after unsuccessful login attempts, and multi-factor authentication for all internal systems. All employees with access to non-public information are required to participate in security awareness training. Creative Compliance performs background checks, including criminal history on all employees.

G. **Electronic Communications Security**

All incoming emails are filtered and scanned for malicious attachments and malicious links at the server, network gateway and client level. Multi factor authentication is utilized for access to email and web services. Mobile device management is enabled for all company owned devices.

H. **Third Party Relationships**

Creative Compliance conducts due diligence into the risks presented by its independent contractors, consultants, and third-party service providers.

I. **Authentication**

All changes to employee, temporary worker, consultant, or contractor privileges are approved by the CTO. The CTO has power entitlements with the Creative Compliance computer systems which are greater than most other users. Access abnormalities are investigated and recorded under the policy's security incident reporting.

J. Privacy Policy

Creative Compliance has an established customer privacy policy and website usage policy for the limited purpose of delivering services our customers have requested. We do not sell, rent or lease customer personally identifiable information to third parties. In the event we share data with trusted partners, such third parties are prohibited from using personally identifiable information and are required to maintain the confidentiality of the information.

5. DATA CONTROLS AND PROCEDURES

A. **Data Classification**

Data is classified in order to properly protect the information assets. The below classifications apply whether the data is stored on company-owned, company-leased or otherwise company-provided systems and media regardless of location.

- **Class I-Public or Non-Classified Information Data** is data not deemed confidential and can be shared publicly without any negative impact on company.
- **Class II- Internal Information Data** is data where external access to this data is to be prevented. If the data becomes public the consequences are not critical and internal employee access does not require any specific entitlements.
- **Class III-Confidential Information Data** is data deemed confidential within company and protected from unauthorized external access. Loss of client or consumer confidence may occur as a result of the data breach.
- **Class IV-Non-Public Information Data** is data including PII and business-related information not publicly available that would cause a material adverse impact to business operations or security if disclosed.

B. **Personal Identifiable Information (PII)**

Creative Compliance recognizes its need to maintain the confidentiality of non-public or Personal Identity Information (PII) and understands that such information is unique to each individual. The PII may come from various types of individuals performing tasks on behalf of the company and includes employees, applicants, independent contractors and any PII maintained on its customer base. The scope of this policy is intended to be comprehensive and will include company requirements for the security and protection of such information throughout the company and its approved vendors both on and off work premises.

C. **Encryption Policy**

Creative Compliance relies on advanced, industry-recognized security safeguards to keep all PII data secure. All data is encrypted both "in motion" and "at rest" wherever possible utilizing 128 and 256 bit advanced encryption standards. All PII stored in system databases is encrypted utilizing Advanced Encryption Standard (AES) and stored for best practices of data at rest.

D. **Data Access Restrictions**

Creative Compliance restricts access to non-public information to only those users for whom access is required to fulfil their job responsibilities.

E. Data Loss Prevention

Data stored on information systems including servers and firm's cloud-based platform will be backed up daily. Backups are encrypted, with redundant local and cloud versions. Logged information generated from each back up will be checked for errors. Random test restores are done regularly to verify backups have been successful, and the CTO or his assign will maintain records demonstrating review of logs and test scores. Prior to the retirement or disposal of any physical media, the CTO or his assign will ensure that the media no longer contains active backup images and that the media's former contents cannot be read or recovered by an unauthorized party. Creative Compliance tests the successful restoration and recovery of key server configurations and data on an annual basis.

F. Right to Deletion/GDRP

Upon a customer's verifiable request, Creative Compliance will delete a customers' personally identifiable information from our records. Creative Compliance, however, may not be able to comply with a customer's request if the personal identifiable information is necessary to:

- Complete the transaction for which the personally identifiable information was collected to provide the service requested, or reasonably anticipated, or otherwise perform the agreed upon services.
- Identify and repair errors that impair existing Creative Compliance intended functionality.
- Exercise a right provided by law or to comply with specific laws, regulations or policies including, but not limited to, the California Electronic Communication Privacy Act.
- Enable Creative Compliance internal uses which are reasonably aligned with a customer's relationship with us, given the context in which the customer provided the information.

G. Data Destruction

When the destruction of data is required pursuant to state and federal law, absent specific regulatory guidelines, Creative Compliance will deploy existing cybersecurity best practices for destruction of data and will maintain the confidentiality of Class IV data assuming the destruction of Class IV data is prohibited.

5. SECURITY INCIDENT REPORTING AND PROCEDURES

A. **Integrity and Confidentiality**

The integrity and confidentiality of business information as well as availability of information systems is critical to Creative Compliance's viability. Creative Compliance has established an enterprise-wide information security policy with supporting procedures in place that set forth how the Creative Compliance will identify and manage its information security risks.

B. Incident Reporting

Creative Compliance has established an incident management policy that addresses incident assessment, escalation, notification, and recovery. In the event of a potential or suspected breach of Creative Compliance information systems or information security the following is a non-exhaustive list of events which trigger reporting:

- Suspected compromise of PII (social security numbers, account numbers, etc...).
- Suspected compromise of login credentials (username, password, etc...).
- Suspected virus, malware or trojan infection.
- Any attempt by a person to obtain a user's password over the telephone or by email.

C. Incident Classification.

- **Security Incident** - any act or circumstance in which there is a deviation from the requirements of this policy is a security related incident. This includes inadvertent disclosure or unauthorized activity that threatens the confidentiality, integrity, or availability of information system resources.
- **Security Breach** - any act or circumstance involving the unauthorized acquisition or access of computerized data that compromises the security, confidentiality, integrity, or personal information is a Security Breach.

6. Security Incident Reporting and Investigation Protocol

A. **Overview**
In the event that a data owner, technology staff member, or Information Technology Services representative identifies a potential security incident, The CTO or his assign will conduct an investigation into the security incident to determine whether there has been a security breach. All investigatory work will be documented within a confidential information security incident report by the assign. If the incident is classified as low/no risk incident appropriate corrective measures will be taken, if the incident is classified as high-risk incident it will be escalated to the senior technology team as a potential security breach for further investigation, upon completion of the investigation, assign will inform cybersecurity committee of the result of the investigation.

B. **Security Breach Notification Protocol**
If it is determined after investigation that a security breach involving notice triggering information has occurred, the Information assign shall notify the CTO, the Cybersecurity Committee, and the firm's General Counsel.

C. **Internal Notifications**
The CTO will initiate the breach notification process and work closely with the technology staff responsible for controlling access to, and security of, the breached system to ensure the appropriate handling of the breach response and inquiries. The CTO will provide guidance to designated employees responsible for responding to breach notification inquiries.

D. External Notification
If it is determined after investigation that a security breach involves data requiring disclosure to a third party such as government agency or merchant bank the CTO shall provide an Incident report to the appropriate entity within in the most expedient time possible following the confirmed breach, not later than 72 hours.

E. **Notification of Affected Individuals**
The CTO or his assign will compile the list of the names of persons whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Additionally, any individuals who are likely to have been affected, such as all whose information had been stored in the files involved, when identification of specific individuals cannot be made. In consultation with the Cybersecurity Committee and the firm's General Counsel the content of breach notification will be established.

F. **Notification Timing**
Individuals whose notice-triggering information has been compromised will be notified in the most expedient time possible, and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notifications will be delivered via email unless government regulations require otherwise.

G. Security Logs
All Security Incidents involving Creative Compliance information systems are logged. The log includes the incident date, summary of incident and steps taken (analysis) to review and resolve the incident.

7. DISASTER RECOVERY AND BUSINESS CONTINUITY PLANS

A. **Overview**

Creative Compliance has established Disaster Recovery and Business Continuity Plans with the objective to respond to the disruptive event as quickly as possible, returning Creative Compliance to business as usual as quickly as possible while preventing loss of Creative Compliance resources including hardware, data and physical IT assets, minimizing related IT downtown and keeping the business running are plan priorities. Creative Compliance tests recovery time objectives for critical systems to restore operations after a cyber-attack or other unplanned outage on an annual basis.

B. **Event Classification**

Events which cause a malfunction of Creative Compliance Information System are classified in order to properly respond to the nature of the event. These include but are not limited to:

- Class I - Network outage or unavailability, including services provided by cloud data service providers.
- Class II - Hardware or software system failures, including services provided by cloud data service providers.
- Class III - Building accessibility, may include physical, water, fire or power issues.
- Class- IV Cybersecurity disruptive event, including ransomware or other cyberattack where data or information may be exposed.
- Class V - Environment catastrophes, including natural disasters, weather events and terrorism.

C. Return to Operation Objectives

While most events will require minimal downtown, the objective is to restore full operations after a major event or computer attack within 72 hours, with a recovery point of no longer than 48 hours data disruption.

Event Class	RTO – PHYSICAL	RTO – CLOUD
Class I	< 4 hrs	< 4 hrs
Class II	< 8 hrs	< 4 hrs
Class III	< 72 hrs	N/A
Class IV	< 72 hrs	TDB
Class V	TBD	TBD

D. Critical Function Recovery Locations

Critical Function	Primary	Alternate Site
System Servers	Data Center Saratoga Springs NY Amazon Webservices - Cloud Azure Webservices - Cloud	Main Office Saratoga NY Amazon Webservices - Cloud Azure Webservices - Cloud
Management Team	Main Office - Saratoga Springs NY	Remote/Home
Support Personnel	Main Office - Saratoga Springs NY	Remote/Home

8. PRODUCT DEVELOPMENT

All software developed is subject to secure system design, coding and testing standards that incorporate appropriate information security controls. All development work shall exhibit a separation between production, development, and test environments, and have a defined separation between development/test and production environments unless prohibited by licensing restrictions or the CTO grants an exception. All applications/programs access paths utilized in development or testing, other than formal user access paths, must be deleted or disabled before software is moved into production and the development process must be documented from the initiation phase, through implementation and ongoing maintenance and security considerations must be noted and addressed through each phase.

9. QUALITY CONTROL & PROCEDURES SUMMARY

Security awareness is important to maintaining the strength of Creative Compliance cybersecurity protections. Creative Compliance monitors regulatory changes relating to security and privacy including introduction of new technologies.

Creative Compliance updates this policy an ongoing basis.