prisma
message to market

Information Security Overview

Prisma Graphic Information Technology is designed and implemented with three primary goals in mind: confidentiality, integrity and availability.

Confidentiality: Information is not disclosed to unauthorized individuals, programs, or processes. Control mechanisms dictate who can access information (authentication) and what actions they can perform to that information (authorization).

Integrity: Information must be accurate, complete, and protected from unauthorized modification. Information must follow controlled change mechanisms, thereby resulting in a high level of confidence in the information.

Availability: Information, systems, and resources are available to users in a timely manner so productivity shall not be affected.

Certifications – SOC2+ and HIPAA Business Associate Compliance

Our physical and Information Security is audited every 24 months by an independent auditor from QCM Solutions. The most recent audit was performed in August 2020. Additionally, our company has been audited and approved as a preferred vendor by two Fortune 50 financial institutions and two Fortune 50 pharmaceutical companies.

Employees are trained annually on our security policies through the use of our Facility Guide. Each employee is background checked and required to complete HIPAA compliance training for Business Associates on a yearly basis.

Physical Security

Our thorough approach to business continuity planning protects data, inventory, facilities and services from all imaginable loss. This planning also allows us to recover from interruptions as quickly as possible and maintain our maximum service levels through any set of circumstances.

Prisma Graphic, located at 2937 East Broadway Road Suite 100, is monitored by ADP Security Company. All Prisma employees must use an assigned access card to enter the facility. The assigned security company keeps digital records of entry and exit from the building based on key card usage.

Any incident involving break-in, vandalism or theft will result in quick and deliberate action by the management team. Management will come to a swift and deliberate course of action based on the incident and its repercussions.

Business Continuity/ Disaster Recovery

Prisma Graphic contracts IO Data Centers to be its primary server location. IO Data has 100% up time SLA service. IO Data provides managed firewalls, multi-protocol data transport, Cross Connect, and blended bandwidth. IO Data is an SAS-70 certified provider.

IO Data Centers provide uninterrupted power and service with redundant power sources, network providers, and 24x7 monitoring and generator power backup systems rated for 30 days without refill. In the event of a power outage at Prisma Graphic headquarters, any business-critical servers and applications hosted in that location would be transferred to the IO Data Center location. In the unlikely event that IO Data Center becomes unavailable, all critical servers hosted in that location would be transferred to the Prisma Graphic headquarters server farm. This transfer process is tested annually and as needed to mitigate risk. Multiple backup methods allow any critical workstation or server to be restored in a matter of a few hours.

Time Warner Telecomm is Prisma Graphic’s internet server provider. TWTC provides 1g fiber connectivity to the physical building. They provide a 200mb point-to-point link with IO Data Center. All routers and security/encryption used on these connections is supplied by TWTC.

Loss of facilities impacting the presses or main offices will be handled as quickly as circumstances allow. Prisma Graphic will minimize any facility or equipment problem’s impact on customers. Third party production equipment and vendors can be utilized to minimize the impact to the business. Temporary office space can be utilized to allow critical personnel to continue working. Phones will be routed to temporary and/or cell phone numbers.

Damage to inventory will be handled as quickly as possible. Back-ups of all critical data will be utilized to reproduce the inventory. Inventory can be replaced within two days by utilizing our network of regional suppliers.

Back-up/Redundancy

All critical servers and workstations are backed up nightly utilizing duplicate Unitrends backup devices. One device is located at the Prisma facility and another at IO data. Both are utilized to port a nightly backup between locations.

Prevention

All access and activity is monitored by the System Administrators and authorized by the executive staff. All employees are required to sign a confidentiality agreement when beginning work at Prisma. Employees are required to follow password control procedures as outlined in our Information Security Policy.

Our Asset and Data Classification policy dictates that all hardware is thoroughly scrubbed and all sensitive data removed before the hardware is disposed of.

Prisma’s web server is segregated from the main network. Because no critical data is housed on the primary network, the possibility of data being corrupted, stolen or destroyed by a malicious hacker is minimal. Any data harmed or stolen in this manner would be inconsequential.

Firewalls and Intrusion Detection methodologies are utilized to prevent intrusion.

Prisma is PCI Level 4 compliant. We have a strong commitment to the PCI DSS requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. Our customers can be confident that they’re protected against the pain and cost of data breaches.

Policies and Procedures

Prisma Graphic operates with a focus on proper policies and procedures that help to ensure the best practices of our staff and the proper protection of our IT Infrastructure and our client’s data. Our thoroughly documented policies outline the proper processes surrounding information security, encryption, acceptable use of technology resources and change management. Policies are reviewed annually or in the event of a major incident. Information Security policies are reviewed by an independent auditor every two years. Our clients are welcome to review any of our policies at the Prisma Graphic offices.

High Security Offerings – HIPAA Compliance

Our production, fulfillment and distribution departments adhere to an even stricter set of guidelines. Our management and staff are focused on protecting data from all malicious intent. All visitors must enter through the front of the building and sign in with our receptionist. Visitors must be accompanied by a Prisma employee at all times. The building is monitored by Safeguard Security Company. Security cameras are positioned at all entry points. Digital video is accumulated for a 30-day period.

In accordance with HIPAA requirements, the physical location where our high security/ePHI work is handled, utilizes a multi-tiered approach to security including:

- Video surveillance, gated entry points and third party monitored alarm systems.
- Employees who work in our high security areas are thoroughly trained and educated in regards to our security policies through the use of our Facility Guide.
    - They also receive ongoing training from supervisors on the proper handling and disposal of sensitive data.
- Individuals with access to the data in electronic form are required to read and acknowledge our IT Security policies for the proper handling and protection of such data.

Utilizing enterprise domain and network best practices, all workstations and users are defaulted to the minimum amount of access rights to complete their job function. Those individuals without a specific business purpose for accessing sensitive data are prevented from doing so by the access controls established in our system.

Firewalls and Intrusion Detection methodologies are utilized to prevent intrusion. All workstations are equipped with Trend Micro. Patches are installed per manufacturer recommendations to ensure that all systems are functioning optimally. Access Control Lists (ACL) are utilized to harden our routers from external access. Logs are regularly reviewed. (FORTIGATE)

Client data is segregated on the network by unique client ID numbers. There is no possibility of co-mingling client data due to the setup and organization of our databases. Clients may provide their confidential or restricted data to us in an agreed upon format. Once Prisma takes control of the data, it is encrypted before it is stored and/or transmitted within our networks.