E2 & GOOGLE CLOUD PLATFORM
SECURITY AND COMPLIANCE YOU CAN TRUST

E2 SHOP SYSTEM

Shoptech takes the responsibility of hosting your data very seriously. That's why we partnered with the most reliable cloud management company in the business, Google Cloud Platform. Google Cloud Platform has unmatched standards within the industry when it comes to security and reliability. Their approach is designed to keep your business running fast, lean, and secure and comes with an industry leading 99.978% Network Uptime Guarantee.

SECURITY OF PHYSICAL PREMISES AND HUMAN RESOURCES

Google designs and builds its own data centers, which incorporate multiple layers of physical security protections. Access to these data centers is limited to only a small fraction of Google employees. Multiple physical security layers are used to protect data center floors and use technologies like biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion systems. Data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training.

Employee Background Checks – Google will verify an individual's education and previous employment, and perform internal and external reference checks of every employee.

Security Training for All Employees – All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. Depending on their job role, additional training on specific aspects of security may be required.

Internal Security and Privacy Events – Google hosts regular internal conferences to raise awareness and drive innovation in security and data privacy, which are open to all employees. Security and privacy is an ever-evolving area, and Google recognizes that dedicated employee engagement is a key means of raising awareness.

Dedicated Security Team – Google employs security and privacy professionals, who are part of our software engineering and operations division. This team is tasked with maintaining the company's defense systems, developing security review processes, building security infrastructure, and implementing Google's security policies.

Dedicated Privacy Team – The Google privacy team operates separately from product development and security organizations but participates in every Google product launch by reviewing design documentation and performing code reviews to ensure that privacy requirements are followed.

Internal Audit and Compliance Specialists – Google has a dedicated internal audit team that reviews compliance with security laws and regulations around the world. As new auditing standards are created, the internal audit team determines what controls, processes, and systems are needed to meet them.

Collaboration with the Security Research Community – Google has long enjoyed a close relationship with the security research community, and greatly value their help identifying vulnerabilities in Cloud Platform and other Google products.

TECHNOLOGY

Data Centers – To keep things running 24/7 and ensure uninterrupted services, Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages.

Environmental Impact – Google reduces the environmental impact of running our data centers by designing and building their facilities. Google installed smart temperature controls, use "free-cooling" techniques like using outside air or reused water for cooling, and redesign how power is distributed to reduce unnecessary energy loss.

Custom Server Hardware and Software – Google's servers and their OS are designed for the sole purpose of providing Google services. Server resources are dynamically allocated, allowing for flexibility in growth and the ability to adapt quickly and efficiently, adding or reallocating resources based on customer demand.

Hardware Tracking and Disposal – Google hard drives leverage technologies like FDE (full disk encryption) and drive locking, to protect data at rest. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to ensure the drive contains no data.

OPERATIONAL SECURITY

Vulnerability Management – Google administrates a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews, and external audits.

Malware Prevention – Google takes these threats to its networks and its customers very seriously and uses a variety of methods to prevent, detect, and eradicate malware.

Monitoring – Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities.

Incident Management – Google has a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority.

Ready to learn more about the E2 SHOP System and how it could work for you? Let's connect soon and start the conversation.

1.800.525.2143
web **www.shoptech.com**

shoptech™