PatternBuilders' Security Practices, Policies & Infrastructure

With Fortune 500 clients in data sensitive industries such as CPG, CES, pharmaceuticals, and health care, PatternBuilders' services, security and data protection are paramount for us. We take security very seriously and have developed a comprehensive set of practices, technologies, and policies to help ensure your data is secure.

If you are currently maintaining your data on personal computers or your own servers, the odds are that we offer a better level of security than what you currently have in place.

This document outlines some of the mechanisms and processes we have implemented to help ensure that your data is protected. Our security practices are grouped in four different areas: Physical Security, Network Security, People, Processes, and Redundancy and Business Continuity.

Physical Security

All PatternBuilders' datacenters are hosted in some of the most secure facilities available today in locations that are protected from physical and logical attacks as well as from natural disasters such as earthquakes, fires, floods, etc. All current and future data centers will, at a minimum, support these security features:

- **7x24x365 Security**. The data centers that host your data are guarded seven days a week, 24 hours a day, each and every day of the year by private security guards.
- **Video Monitoring**. Each data center is monitored 7x24x365 with night vision cameras.
- **Controlled Entrance**. Access to PatternBuilders' data centers is tightly restricted to a small group of pre-authorized personnel.
- **Undisclosed locations**. PatternBuilders' servers are located inside generic-looking, undisclosed locations that make them less likely to be a target of an attack.
- **Bullet-resistant walls**. PatternBuilders' servers are guarded safely inside bullet-resistant walls.
- **No Shared Infrastructure**. Unlike most SaaS solutions, PatternBuilders' customers' data is never pooled on the same operating system instance, providing both predictable performance and increased security.

Network Security

Our network security team and infrastructure helps protect your data against the most sophisticated electronic attacks. The following is a subset of our network security practices. These are intentionally stated in a very general way, since even knowing what tactics we use is something hackers crave. If your organization requires further detail on our network security, please contact us.

- **128/256-bit SSL**. The communication between your computer and our servers is encrypted using strong 128-bit keys (256-bit keys in many cases). What this means is that even if the information traveling between your computer and our servers were to be intercepted, it would be nearly impossible for anyone to make any sense out of it.
- **IDS/IPS**. Our network is gated and screened by highly powerful and certified Intrusion Detection / Intrusion Prevention Systems.
- **Control and Audit**. All accesses are controlled and also audited.
- **Virus Scanning**. Traffic coming into PatternBuilders' servers is automatically scanned for harmful viruses using state of the art virus scanning protocols which are updated regularly.

People Processes

Designing and running data center infrastructure requires not just technology, but a disciplined approach to processes. This includes policies about escalation, management, knowledge sharing, risk, as well as the day-to-day operations. PatternBuilders' security team has years of experience in designing and operating data centers and continually improves its processes over time. PatternBuilders has developed world class practices for managing security and data protection risk.

- **Select Employees.** Only employees with the highest clearance have access to our data center data. Employee access is logged and passwords are strictly regulated. We limit access to customer data to only a select few of these employees who need such access to provide support and troubleshooting on our customers' behalf.
- **As-Needed Basis.** Accessing data center information as well as customer data is done on an as-needed only basis, and only when approved by the customer (i.e. as part of a support incident), or by senior security management to provide support and maintenance.

Redundancy and Business Continuity

One of the fundamental philosophies of hosted solutions is the acknowledgment and assumption that computer resources will at some point fail. We have designed our systems and infrastructure with that in mind.

- **Power Redundancy.** PatternBuilders configures its servers for power redundancy – from power supply to power delivery.
- **Internet Redundancy.** PatternBuilders is connected to the world—and you—through multiple Tier-1 ISPs. So if any one fails or experiences a delay, you can still reliably get to your applications and information.
- **Redundant Cooling and Temperature.** Intense computing resources generate a lot of heat, and thus need to be cooled to guarantee a smooth operation. PatternBuilders' servers are backed by N+2 redundant HVAC systems and temperature control systems.
- **Backups.** Customer data is backed up daily. A weekly backup is stored in a separate physical location for Disaster Recovery and Business Continuity purposes.
- **Fire Prevention.** PatternBuilders data centers are guarded by industry-standard fire prevention and control systems.

Additional Information

While we cannot list all the details of our infrastructure for security reasons, rest assured that PatternBuilders' security practices, policies and infrastructure are proven and reliable.