PRISMHR

PrismHR Security

Cybersecurity issues are a reality for virtually all businesses and that is why we take them so seriously. PrismHR has maintained SOC 2 compliance since 2018, and we continue to take steps to strengthen our security protections and business continuity processes.

To safeguard the data of HR service providers and the businesses they support, PrismHR is committed to continuously enhancing our security practices and protocols.

Information Security Compliant

PrismHR maintains System and Organization Controls Type 2 ("SOC 2") compliance. This means PrismHR has demonstrated to an independent auditor that the PrismHR platform is designed to keep our customers' data secure.

Application Security

PrismHR employs multiple features to prevent unauthorized access to the system and your data, including multi-factor authentication, strict password rules, IP address control, and role-based security.

Data Monitoring & Encryption

Our platform is actively monitored 24/7/365 to protect against data breaches and cyberattacks. Access to your HR technology requires a secure connection. And all data is encrypted before being sent to or stored in the cloud to prevent it from being captured while in transit or at rest.

The EDR solution also includes 24/7 managed response by a team of cyber defense experts. This combination of sophisticated software with human oversight is designed to address a constantly evolving landscape of cyber threats.

All data in the PrismHR platform is encrypted before being sent to or stored in the cloud to prevent it from being captured while in transit or at rest.

Zero Trust Strategy

PrismHR will move further toward a zero trust approach—a leading cybersecurity methodology—to reduce risk and ensure users across the system have the appropriate level of access. Zero trust incorporates what users (including authorized ones) are doing

inside the system and authenticates users as they move through the system based on access level and behavior patterns.

Under a zero trust approach:

- Users have only the level of access they need to do their jobs
- Requests for additional privileges will trigger a process to authenticate the user's identity and/or validate the need for access
- Access to certain areas of the system may only be turned on temporarily for a user
- Validating a user's identity may require a combination of login credentials, multi-factor authentication, IP verification and behavior

Business Continuity

PrismHR maintains and regularly tests business continuity, incident response, and disaster recovery plans. This process is designed to detect, resolve, and guide recovery from a security breach, and identify opportunities for improvement.

As part of this process, we are bolstering our disaster recovery with processes and technology that allow us to restore system access more quickly from a cyber incident.

First, we are adding failover environments that are disconnected from production which will shield them from being impacted (like a wide moat that a bad actor can't cross). Second, we are limiting how often failover environments connect to the internet (e.g., periodically for backups) instead of keeping them constantly online. This provides an additional layer of protection which will allow us to recover far more quickly from any future incident.

Data Center Security

PrismHR is hosted in a private cloud at a leading enterprise cloud provider. Our cloud provider adheres to the latest security, control and performance standards including ISO 27002 and 27001, PCI-DSS, SSAE16, SOC 1, 2, and 3 compliance, and Privacy Shield and Content Protection and Security Standard requirements. The provider is subject to regular third-party audits.

Continuous Improvements

PrismHR is committed to continuous improvements and implementing learnings that increase our security posture beyond our existing high standard. That includes adding new state-of-the-art security tools and procedures.