iSolved®

THE POWER & STRENGTH OF iSOLVED

- Over 3 million employees
- Over 45,000 employers
- Supported & developed by a 30-year-old company
- iSolved Marketplace for additional integrated products and services
- One database for HR, payroll, time & benefits
- Fastest market share growth in HCM space
- Serviced by regional service bureaus for an exceptional customer experience

Regulatory Compliance

Customers are responsible for complying with local, state, federal and foreign laws where applicable. These include many that are related to data privacy and transmission of data, even when a service provider is in possession of that data. iSolved® maintains a formal and comprehensive program designed to ensure the security of customer data, protect against security threats and prevent unauthorized access to the data of its customers. A key indicator of that formal program is an ongoing review process by third-party auditors.

iSolved, along with its data center service provider, uses the Statement on Standards for Attestation Engagements (SSAE) No. 16. as the basis of this external audit and review. SSAE 16 was finalized by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) in Jan. 2010. SSAE 16 effectively replaced the SAS 70 as the authoritative guidance for reporting on service organizations effective June 15, 2011. Completion of the SSAE 16 audit gives companies confidence when conducting business with service providers like iSolved. Specifically, a SOC II Type II report for the iSolved Network system is completed annually during the month of August.

iSolved maintains a formal and comprehensive program designed to ensure the security of customer data, protect against security threats and prevent unauthorized access to the data of its customers.

A copy of the audit report is available to partners and customers under a non-disclosure agreement. In addition, iSolved can provide a statement to attest that all operational controls identified in its SSAE 16 audit remaining in continuous operation since the last audit date (ie, a “gap” letter).

Physical & Logical Security

iSolved houses its production systems in state-of-the-art data centers designed to host mission-critical computer systems with fully redundant subsystems and compartmentalized security zones. iSolved data centers adhere to the strictest physical security measures:

Requires multiple layers of authentication before access is granted to the server area

Critical areas require two-factor biometric authentication

Camera surveillance systems at critical internal and external entry points

On-site security personnel monitoring 24/7

Background checks required for all personnel with access to the data center

All logical access to the systems in the data centers is highly restricted through the use of a segregated Active Directory domain. iSolved IT Operations use security best practices such as "least privilege" to harden individual servers and minimize change via regularly scheduled maintenance windows. Security specific updates are applied at least monthly, based on the vendor's release schedule.

Logical access to the iSolved application is enforced through role-based security which is managed by the client. Policies that govern password expiration, password complexity, password reuse, and account staleness are strictly enforced for all user accounts regardless of role.

Data Segregation

The iSolved application is a multi- tenant SaaS application. **Multi-tenancy is a key differentiator from other hosted HCM solutions.** It enables multiple customers to share one physical instance of the iSolved system while isolating each customer's data. iSolved accomplishes this through an object layer that is always linked to one specific customer. All instances of application objects (employee, legal company, pay group, etc) are created with data restricted to one customer.

The iSolved system maintains links between each user and each customer. When a user requests data, the system automatically uses the customer specific objects that have already been subject to the filters restricting data to a particular customer.

Two-Factor Authentication

The primary means for authentication to the iSolved application is username/password. However, the system keeps track of "authorized" locations (IP addresses) where the user credentials are valid.

If a user's credentials are used from an "unauthorized" location, the user will be sent an additional code to the email address on record. This code needs to be entered to gain access to iSolved . If successful, that location will be added to the authorized list.

Data at Rest (Database Security)

iSolved encrypts customer and employee data that is considered Personally Identifiable Information (PII). This encryption occurs within the application itself before any data is stored in the database. Likewise, decryption of that data occurs "just in time" at the point that it needs to be rendered on a page or used by the application.

This is a unique design characteristic of the iSolved technology which relies on the latest Advanced Encryption Standard (AES) algorithms. By selectively encrypting data, iSolved is able to use standard relational database technology, but avoid any detrimental performance impact that complete database encryption might cause.

Data in Transit (Network Security)

Users' access to iSolved via the Internet is protected by Transport Layer Security (TLS). Certificates are actively managed to ensure they use and support the latest encryption and cipher technology. This secures network traffic from passive eavesdropping, active tampering or forgery of any messages.

iSolved also employs proactive security measures such as perimeter defense and network intrusion detection/ prevention systems. Vulnerability assessments are performed on the iSolved system by external resources on an annual basis.

Data Backups

iSolved's production database is backed up to disk on a weekly rotation schedule. This entails a weekly full backup, a nightly differential backup and transaction log backups every hour. This procedure allows for recovery to a "point in time" in the event of a local database system failure. This procedure is designed so that the database can be recovered with as few committed transactions lost as is commercially practicable. In addition, these backups are replicated off-site for additional safe keeping for a period of 14 days.

The production system consists of a distributed set of servers that are actually built on virtualization technology. The image of each server is backed up to disk on a nightly basis and replicated off-site in a similar manner as the database. In the event of a local hardware failure, the virtualization layer allows for any iSolved server to be moved to a surviving node within an overall N+2 architecture.

Disaster Recovery

In addition to the resources backed up locally, iSolved replicates the entire production environment to another production data center over 300 miles away. In the event of a disaster where the outage is estimated to be greater than a predefined duration for the type of outage, iSolved will execute its business continuity plan. This plan uses the replicated images and databases to reconstitute a running production instance of the iSolved system. Customers will have access to this new location once it becomes available.

The iSolved plan for recovery includes a Recovery Time Objective (RTO) of eight hours and a Recovery Point Objective (RPO) of less than 15 minutes.

In addition to the resources backed up locally, iSolved replicates the entire production environment to another production data center over 300 miles away.