candoor
PAYROLL & HCM

Security and Reliability

Delivered through the most powerful cloud computing environment, Microsoft Azure™

- Over 6 million employees
- Single code base for HR, payroll, time and benefits
- Over 168,000 employers
- Fastest market share growth in HCM space
- isolved University, with training courses and quick help guides
- Transforming employee experience for a better today and a better tomorrow

Azure is the Powerhouse for Security

isolved maintains a formal and comprehensive security program to protect customer data and prevent potential threats. Third-party auditors regularly review the program, which includes compliance with local, state, federal and foreign data privacy and transmission laws - even when a service provider is in possession of that data.

isolved and Microsoft use the Statement on Standards for Attestation Engagements (SSAE) 18 as the basis of this external audit and review. SSAE 18 is a standard maintained by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA), replacing SSAE 16 and SAS 70 as the authoritative guidance for reporting on service organizations since May 1, 2017. isolved completes its annual SOC1 Type 2 report in August for the previous 12 months. Three SOC 1 reports are produced for the isolved SaaS platform, payroll and tax filing services, and the legacy TimeForce II SaaS solutions.

Audit reports are available to customers and prospects with a current master support agreement (MSA) or under a mutual non-disclosure agreement. isolved can provide a statement to attest that all operational controls identified in the SOC I report remain in effect since the last audit date (i.e., a "gap" letter).

isolved is hosted and protected by the biggest and most trusted name in cloud computing,

Microsoft Azure™

Multiple independent third-party assessments (including Corsis) of the isolved technology, development processes, and infrastructure are conducted regularly to confirm isolved's market-leading position.

**Microsoft product names, brands, and other trademarks are the property of their respective trademark holders. These trademark holders are not affiliated with isolved.*

isolved Network
Certified Partner

Candoor Payroll & HCM Inc
2504 Veterans Memorial Pkwy S., Ste 1
Lafayette, IN 47909

candoor
PAYROLL & HCM

Physical & Logical Security

isolved's production systems are hosted on Microsoft Azure's cloud infrastructure in a state-of-the-art data center. It is designed to host mission-critical systems, with redundant subsystems and compartmentalized security zones. Microsoft's Azure data centers strictly adhere to physical security measures, including:

- Virtual access to servers requires multiple layers of authentication
- On-site security personnel monitoring 24/7 and integrated alarm systems
- All data center personnel must pass background checks
- Critical infrastructure requires two-factor biometric authentication
- Camera surveillance systems at critical internal and external entry points
- World-class Disaster Recovery and High Availability Architecture to maximum resiliency

Physical access to Azure Datacenters is highly restricted, including logical access to isolved environments, systems, and hosted platforms in these data centers. This is managed through various administrative and logical controls. Our Cyber Security and IT Operations teams follow multiple industry best practices, including the National Institutes of Standards and Technology (NIST) cybersecurity framework, the IT Infrastructure Library (ITIL) framework for servicing and management, the Open Web Application Security Project (OWASP) guidelines for cloud and secure code development, as well as several others. These frameworks and best practices enable isolved to drive toward worldclass solutions for the policies that support our differentiating resiliency, servicing, and security.

Data Segregation

The isolved application is a multi-tenant SaaS platform that enables customers to leverage the highly scalable modules of our cloud architecture, utilizing them as needed and on demand. Every customer's data is segregated and segmented into its own group and access control mechanisms. isolved accomplishes this through a data management layer that is always scoped to one specific customer, ensuring that all instances of the application objects (employee, legal company, pay group, etc.) are created with data restricted to that customer.

Additionally, each user account is maintained within the context of a customer, and the system automatically uses the customer-specific objects that have already been subject to filters when a user requests data. Role-based filters can further restrict the scope all the way down to the employee level.

Two-Factor Authentication

The isolved application uses username/password authentication and tracks "authorized" client devices where the user credentials are valid. "Unauthorized" device use triggers two-factor authentication, with a code sent to the user via email or text. This code needs to be entered to gain access to isolved. Successful authentication will authorize the device subject to other password policies.

Data at Rest (Database Security)

isolved encrypts client and employee data that is considered Personally Identifiable Information (PII) within the application before any data is stored in the database. The decryption of that data occurs "just in time" when it needs to be rendered on a page or used by the application.

This is a unique design characteristic of isolved's technology and uses the latest Advanced Encryption Standard (AES) algorithms to selectively encrypt data. isolved can use standard relational database technology but avoid any detrimental performance impact that complete database encryption might cause.

Data in Transit (Network Security)

isolved uses Transport Layer Security (TLS) to protect user access via the internet. Websites are configured and certificates managed to support the latest encryption and cipher technology, securing network traffic from passive eavesdropping, active tampering or forgery of any message traffic.

isolved also employs proactive security measures, such as perimeter defense and network intrusion detection/ prevention systems. Vulnerability assessments are conducted annually by external auditors. All network traffic internally at isolved, across all our facilities and for all remote users, is encrypted.

Data Backups

isolved production databases are regularly backed up on multiple schedules and across multiple regions and availability "zones". These backups include a weekly full backup, a nightly differential backup and hourly transaction log backups. This procedure allows for recovery to a specific "point in time" in the event of a local database system failure. This process is designed to restore the database with as few committed transactions lost as is commercially practicable. These backups are also replicated to another data center in the Azure cloud. All backups in our recovery vaults are also "immutable" meaning that each backup cannot be manipulated or updated between each full back-up.

The isolved production system is a distributed set of servers built entirely on cloud hosted technology. In the event of a hardware (host) failure, the architecture and hosting configuration enables the failover to a surviving or redundant server within the highly available Azure hosting environment and our isolved cloud-based architecture. The proof of the sustained availability and reliability of the isolved platform is in our quarterly uptime reporting as well as in our contractual Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

Disaster Recovery

In order to ensure continuity of operations in case of a disaster, isolved replicates its entire production environment to another Azure region almost 3,000 miles away (U.S. East to West Coast). In the event of a disaster declaration, where the business risk of the outage is more significant than the technical risk of a failover, isolved will execute its disaster recovery plan. The failover process is tested semi-annually and can occur in under 1 hour, with less than 5 minutes of data loss. By employing this strategy, isolved can maintain business continuity and ensure that critical systems remain operational in the face of potential disruptions.

In addition to the resources backed up locally, isolved replicates the entire production environment to another production data center almost 3,000 miles away.

isolved includes a contractual Recovery Time Objective (RTO) and a Recovery Point Objective (RPO) as defined in the master service agreement (MSA).

An independent third-party assessment (Corsis) of the isolved technology, development processes, and infrastructure was conducted in May 2019 and confirms isolved's market-leading position.

Contact us to learn how we are working hard to keep your data secure! **765-474-7326**

isolved Network
Certified Partner

Candoor Payroll & HCM Inc
2504 Veterans Memorial Pkwy S., Ste 1
Lafayette, IN 47909

candoor
PAYROLL & HCM