



## Power & Strength.

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



Over 5 million employees



Single code base for HR, payroll, time & benefits



Over 145,000+ 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 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. 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, along with its cloud service provider Microsoft, uses 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). SSAE 18 replaces SSAE 16 and the older SAS 70 as the authoritative guidance for reporting on service organizations, effective May 1, 2017. Completion of the SSAE 18 audit gives companies confidence when conducting business with service providers. isolved completes its annual SOC 1 Type 2 report in August, covering the 12 months preceding the report date. Three SOC 1 reports are produced to cover the isolved SaaS platform, the isolved payroll and tax filing services, and the legacy Timeforce II SaaS solutions.

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

isolved is hosted and protected by the biggest and most trusted name in cloud computing,  
**Microsoft Azure™**

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



isolved Network  
Certified Partner

32 Tioga Way, Marblehead, MA 01945  
www.commpayhr.com  
sales@commpayhr.com | (978) 599-1500

COMMONWEALTH  
PAYROLL & HR








A copy of these audit reports is available to partners, customers, and prospects with a current master support agreement (MSA) or under a mutual non-disclosure agreement. In addition, 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).

## Physical & Logical Security

isolved houses its production systems in a state-of-the-art virtual private data center within the Microsoft Azure cloud infrastructure. It is designed to host mission-critical systems with fully redundant subsystems and compartmentalized security zones.

Microsoft’s Azure 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
-  Background checks required for all personnel with access to the data center
-  Camera surveillance systems at critical internal and external entry points
-  On-site security personnel monitoring 24/7

All logical access to the isolved platform in these 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.

Logical access within 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 platform while isolating each customer’s data. isolved accomplishes this through an object layer that is always scoped to one specific customer. All instances of the application objects (employee, legal company, pay group, etc.) are created with data restricted to that one customer.

The isolved application maintains each user account within the context of a 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 specific customer. Additional role-based filters further restrict the scope all the way down to the employee level, if necessary.

## Two-Factor Authentication

The primary means of authentication to the isolved application is username/password. However, the system keeps track of “authorized” client devices where the user credentials are valid.

If a user’s credentials are used from an “unauthorized” device, the user is required to use two-factor authentication. The user will be sent an additional code via email or text to an email address or mobile phone number on record. This code needs to be entered to gain access to isolved. If successful, that device will be “authorized” subject to other password policies.

## 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 isolated technology and uses the latest Advanced Encryption Standard (AES) algorithms. By selectively encrypting data, isolated can 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 isolated via the internet is protected by Transport Layer Security (TLS). Websites are configured and certificates 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 message traffic.

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

## Data Backups

isolated production databases are 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 to another data center in the Azure cloud.

The production isolated system is a distributed set of servers that is built entirely on virtualization technology. The image of each server is replicated to separate cloud storage on a continual basis. In the event of a local hardware (host) failure, the virtualization layer allows for any isolated server to be moved to a surviving host within the highly redundant Azure cloud.

## Disaster Recovery

In addition to the resources backed up locally, isolated replicates the entire production environment to another Azure data center 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 greater than technical risk of a failover, isolated will execute its disaster recovery plan. This plan relies on Azure-provided recovery services, which replicate all virtual machine images and databases to a secondary cloud data center. Customers will have access to this new location after startup procedures are followed and verification testing is successful. The failover process is tested semi-annually and can occur in under 1 hour, with less than 5 minutes of data loss.

*isolated 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 isolated technology, development processes, and infrastructure was conducted in May 2019 and confirms isolated's market-leading position.*

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

*Transforming employee experience for a better today and a better tomorrow.*



32 Tioga Way, Marblehead, MA 01945  
www.commpayhr.com  
sales@commpayhr.com | (978) 599-1500

