



## Locked & Secured: How isolated Safeguards Employer & Employee Data

There's no more sensitive data than people data. With the increasing sophistication of cybercrime and fraud, the importance of security and risk management has never been more important.

isolated has spent more than 35 years safely and securely delivering human capital management (HCM) technology, with millions of dollars in ongoing cybersecurity investment.

**"Security and compliance are not secondary investment areas for isolated. They are primary investment areas for isolated."**

Mark Duffell  
Chief Executive Officer, isolated

### Here are highlights of isolated's ongoing investments in security:

- **Hosted on Microsoft Azure™**, isolated People Cloud™ customers benefit from multi-layered security, state-of-the-art protection, customized hardware and firmware, and a global team of over 3,500 Microsoft cybersecurity experts dedicated to safeguarding business assets and data hosted on Azure.
- **Committed to current and future compliance standards**, isolated maintains best-in-class certifications, including SOC 1 and SOC 2 Type II audits.
- **Encrypted data** reduces the chance it can get in the wrong hands. isolated encrypts data within People Cloud using Transport Layer Security (TLS) for personal identifiable information (PII) in transit and Advanced Encryption Standard (AES) for data at rest.
- **Secured and segmented**, deployments use multiple multilocation immutable backups, dedicated environments, firewalled applications, verified disaster recovery plans, just-in-time access and standardized configurations to reduce risk.
- **Guided by the highest standards**, including the National Institute of Standards Technology (NIST) cybersecurity framework and ITL 4.0, isolated remains committed to cutting-edge cybersecurity investments.
- **Standardized multifactor authentication (MFA)** is used to reduce the risk of account takeovers by bad actors by requiring MFA at login. Please keep in mind that employees and employers should never share their login credentials within anyone, including multifactor authentication codes. isolated will never call and ask for it.



connect@coastalpayroll.com | 858-565-2123



- **Required background checks** and regular training for all employees, ensures isolated hires and retains vetted staff.
- **Tenured executives** hold the roles of full-time chief information security officer, chief technology officer and chief compliance officer to ensure administrative, technical, and physical safeguards and structures are in place for privacy and vendor risk management.
- **Embedded within proprietary and partner software**, isolated continuously monitors, detects and prevents security threats.
- **Dedicated to providing comprehensive information** about governance, risk, and compliance (GRC) processes and controls, the regularly updated vendor Trust Center serves as a single resource for customers, partners, and prospective customers.
- **Established to support the company's compliance program**, the Compliance Committee facilitates the exchange of information, monitors risk metrics, provides regulatory updates, collaborates on cross-functional risk management projects, enhances confidential communication about corporate risks and mitigation strategies, and monitors compliance across the organization.



#### Administrative safeguards:

- Training
- Documentation
- Practices
- Policies
- Procedures

#### Technical safeguards:

- Firewalls
- Multi-factor authentication
- Encryption
- Access control

#### Physical safeguards:

- Security badges
- Locked doors
- Access cards
- Biometric access controls
- Video cameras
- Surveillance cameras
- Motion sensors
- Fire suppression
- Environmental controls (e.g., HVAC and humidity controls)

**To learn more about isolated's ongoing investments in security, please visit our Trust Center by scanning the QR code or going directly to [isolatedhcm.com/trust-center](https://isolatedhcm.com/trust-center).**



\*Microsoft product names, brands, and other trademarks are the property of their respective trademark holders. These trademark holders are not affiliated with isolated. Disclaimer. The information provided herein is for general informational purposes only and is not intended to be legal or other professional advice, including data privacy and security advice. All information discussed is of a general nature and does not address the circumstances of any particular individual or entity. We make no representation that the content will guarantee prevention of cyber incidents and disclaim all liability for actions you take or fail to take based on any content we provide. There is no form of relationship formed by any use of this information. The accuracy, completeness or adequacy of the information is not guaranteed, and isolated assumes no responsibility or liability for any errors or omissions in the content. It is not a substitute for legal advice or any other professional advice, including data privacy and security and you should not rely on it as such. You should consult with an attorney, or other appropriate professional for advice regarding your specific situation.



connect@coastalpayroll.com | 858-565-2123

