Workrig Cloud Security

As a provider of enterprise cloud applications for human resources, we believe in futuristic thinking to keep up with the technological development and its practical implementation for our clients.

Protecting our customers' data is our prime focus and we emphasis more on delivering industry –best practices, with our forever evolving software products.

Be sure the data you store in cloud is safe.

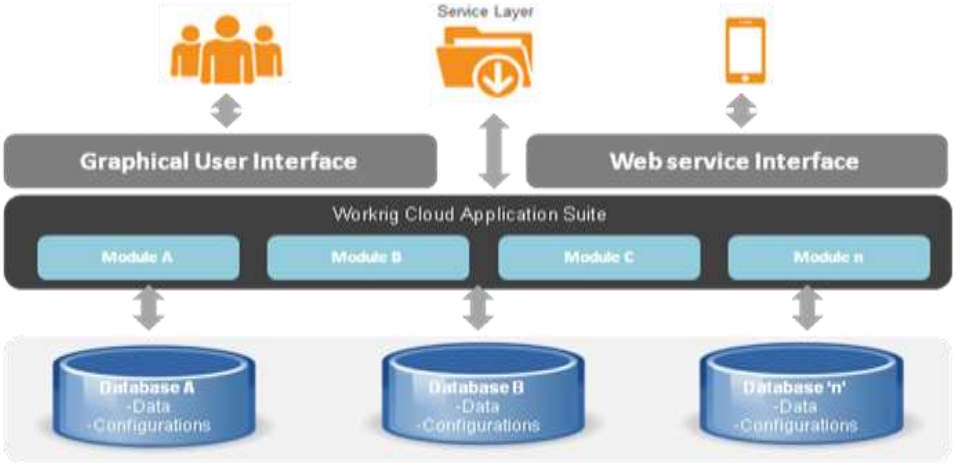
At Workrig we take into consideration, data security at a very early stage of the product development. The same is considered while architecting the product and all possible scenarios are explored in keeping with its deployment objective of hosting on a cloud infrastructure.

Workrig is designed on Multi-tenant architecture, therefore mitigating any issues that could arise due to Data- Mingling. A software level design was achieved by providing Access Control Level's to the user, therefore reducing any data-violation by visibility, at any levels.

What resulted was a complete application-level security infrastructure supporting: role, data security, data encryption and auditing. These comprehensive security features enabled the application architect to implement security policies that would protect your valuable corporate data from inappropriate or unlawful access while enabling your trusted employees to effectively use the software.

Workrig Technology Features

- Multi tenant Architecture
- SSL certification/256bit AES encryption
- Automatic data backup across two DR Sites, in West Coast & Indian Server's
- Quick Processing
- Easy-to-use & Scalable
- Most competent accurate and ready to use
- Execution speed



Single Login , across Web and mobile apps

One Application for all customers, thereby, updates are applicable to all customer. Single Version for all

Distinct Database for each customer:
- No data mingling
- Custom Configuration & customization potential
- Scalable and secure multi-tenant model

Secure Socket Layer (SSL) technology (256 bit AES), which protects application information accessed through a browser using server authentication and data encryption

Workrig's Cloud Encryption solutions include secure data and intellectual property that form end point to cloud data security.

One-stop solution for organizations that rely on technology for the critical HRMS processes: Beginning from hiring, on-boarding, training, performance management, payrolls, compliances, timesheet, leave management till off-boarding and exit.

If you'd like to spend more time truly improving the overall work environment for your employees, you want to help company management find ways to save on workforce-related costs and time, Then, Workrig Cloud platform provides multi-tenant, robust and scalable web-enabled solutions. It allows organizations to simply compose rather than laboriously code solutions. Workrig provides an integrated software solution for managing your organization's workforce.

Security technologies & methods

Data Segregation

Workrig is a multi-tenant Software-as-a-Service (SaaS) application. Multi-tenancy is a key feature of Workrig that enables multiple customers to share one physical instance of the Workrig system while isolating each customer tenant's application data.

Workrig accomplishes this through the Workrig object management . Every user ID is associated with exactly one tenant, which is then used to access the Workrig application. All instances of application objects (such as Organization, Employees, etc.) are tenant based, so every time a new object is created, that object is also irrevocably linked to the user's tenant. The Workrig system maintains these links automatically, and restricts access to every object based on the user ID. The Workrig system restricts access to objects based on the user ID and tenant. When a user requests data, the system automatically applies a tenancy filter to ensure it retrieves only information corresponding to the user's tenant.

Encryption of Data at Rest (Database Security).

Workrig encrypts every attribute of customer data within the application before it is stored in the database. This is a fundamental design characteristic of the Workrig technology. Workrig relies on the Advanced Encryption Standard (AES) algorithm with a key size of 256-bits.
All data inserts, updates, and deletes are committed to a persistent store on a PostgreSQL database.

Encryption of Data in Transit

Workrig is on 256bit AES encryption. SSL Certificates digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser.

Workrig is on 256bit AES encryption. SSL Certificates digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser.

World Class Data Centers, equipped with Physical and Networking Security

Workrig hosts its Production systems in state-of-the-art facilities, globally renowned Data Centers and Services, for hosting enterprise level applications. Workrig hosts applications with AWS and IWeb. For more about Physical and Networking security measures, one can read the following articles:

https://aws.amazon.com/security/
https://aws.amazon.com/compliance/
https://iweb.com/firewalls

Data Backups

Workrig's master production database is replicated in real-time to a slave database maintained at an offsite data center. A full backup is taken from this slave database each day and stored at the offsite data center facility. Workrig's database backup policy requires database backups and transaction logs to be implemented so that a database may be recovered with the loss of as few committed transactions as is commercially practicable. Transaction logs are retained until there are two backups of the data after the last entry in the transaction log. Database backups of systems that implement interfaces must be available as long as necessary to support the interfacing systems. This period will vary by system. Backups of the database and transaction logs are encrypted for any database which contains customer data.

Cloud Data & Disaster Recovery

Workrig warrants its service to its standard Service Level Agreement (SLA). The SLA includes a Disaster Recovery (DR) plan for the Workrig Production Service with a Recovery Time Objective (RTO) of 12 hours and a Recovery Point Objective (RPO) of one hour. The Recovery Time Objective is measured from the time the Workrig Production Service becomes unavailable until it is available again. The Recovery Point Objective is measured from the time that the first transaction is lost until the Workrig Production Service became unavailable.

To ensure Workrig maintains these SLA commitments, Workrig maintains a DR environment with a complete replication of the production environment. In the event of an unscheduled outage where the outage is estimated to be greater than a predefined duration, Workrig executes its DR plan. The PostgreSQL database is replicated to the DR data center, new OMS instances are started in the DR data center, and customers are redirected to the DR data center.

The DR Plan is tested at least every six months.