Epic Solutions

Protecting your Data in the Cloud

An Under the Hood look at epicCare

Table of Contents

An Under the Hood look at epicCare

Cloud computing is used by many organisations to help address their business requirements. Why? Because modern cloud computing solutions just make sense when you compare them to traditional, time-consuming, and costly on-premises solutions. Among other things, cloud computing can help you reduce capital expenditures, minimize application deployment times, eliminate maintenance tasks, and refocus your staff on adding value to your core business.

The same is true for security in the cloud. Cloud providers have highly skilled security teams and economies of scale to invest in the latest security technologies. Cloud providers are motivated to ensure customer security success since this is foundational to the cloud business. In many cases, the security resources and reassurances that a cloud provider offer exceed those that organizations can afford independently.

Even with all of these compelling benefits of moving to the cloud, it’s important that you are confident that your cloud provider has the world-class security and privacy solutions that can adequately protect your data. So what does it take to trust a cloud? Like any other system, a cloud provider must protect your assets from internal and external threats, maintain the privacy of your data, remain available and reliable, and perform consistently.

A good cloud solution can be measured by the level of control you maintain over your assets. In addition to understanding your specific risk tolerance, data security, data privacy, and regulatory compliance requirements, you should carefully choose a service that can provide you with adequate controls for meeting your business requirements.

This paper explains how epicCare uses cloud solutions to manage and protect your assets. First, you’ll learn about our commitment to earning and maintaining your trust. Next, you’ll discover the core operational and functional security measures that our platforms use to protect your data. Finally, you’ll explore the built-in features of our services that you can draw on to build applications that satisfy even the most stringent security requirements.

Your Trust, Our First Concern

Trust has always been a core principle at epicCare since the company's inception in 2000. With this core belief in mind, let's learn more about what epicCare does to ensure that your data remains secure, private, and available.

How We Certify Our Business Practices

epicCare's services are certified as compliant with some of the most rigorous, industry-accepted security, privacy, and reliability standards.

Our data centres operated by Strencom as an ISO27001 Certified service. It is an On-Demand Cloud service, which provides access and control over your cloud infrastructure through a browser based interface. It is designed for enterprise computing applications with performance, reliability, and security to the fore.

- Hosted in Ireland - Guaranteed. You data will never leave the data centre
- Custom built Cloud on VMware Vcloud
- Design, Build and Execute Physical to Cloud or Virtual to Cloud
- Support for specific applications
- Built on secure foundations
- IBM Storwise V7000 Servers and Storage
- VMware Hypervisor
- Cisco Backbone
- Brocade Fibre Channel Fabric
- Physical & Logical security of data

KeepItSafe provides a fully managed and monitored service tracking errors, missed backups, or unusual activity. At the same time, KeepItSafe engineers proactively monitor all backups 24/7 to support and augment the technology, and establish contact to resolve any issues.

Additional protocols include:

- Proactive Backup Monitoring
- All unusual activity flagged
- Quick, decisive intervention and customer notification
- Data encrypted in transit and at rest
- 24-hour data-centre security

How We Operate Internally

epicCare's commitment to security, privacy, reliability, and trust permeates the entire company. It starts at the very top with executives who lead teams responsible for the implementation of comprehensive information security governance policies

Employees – All of our employees receive information security and privacy training. Employees that handle data receive additional training specific to their roles.

- Security staff – We have specialised security staff and access to external highly skilled security professionals as needed.
- Assessments – We regularly conduct vulnerability assessments (for example, audits and reviews by security professionals) as well as working with our data centre partners to manage external threats.
- Protocols – Detailed internal protocols dictate how we detect, investigate, and respond to security and privacy incidents.

How We Build Secure Products

We build software benchmarking against OWASP recommendations and other security best practices into the system development processes at all stages. Here's a summary of some of the development phases we go through.

- Design phase – Guiding security principles and required security training help ensure that our technologists make the best security decisions possible. Assessing threats to high-risk features helps us identify potential security issues as early in the development lifecycle as possible.

- Coding phase – We address standard vulnerability types with secure coding patterns and anti-patterns, and use static code analysis tools to identify security flaws. Software releases include a code review and fix all our significant security findings before our applications go live.

- Testing phase – Our internal staff and independent security consultants use third-party tools, proprietary tools, and manual security testing to identify potential security issues.

- Ongoing retest– Based on new learning and product development, previous releases are recursively tested.

How We Fortify Our Data Centres

All data is stored in a physically secure dedicated data centre facility which includes connectivity to multiple Tier 1 providers and clean power supply through UPS, FM-200 Fire Suppression, 24 x 7 Monitored NOC, 99.98% Uptime SLA and Monitored Data Backups.

Data is backed up to locations in multiple data centres, operating under ISO27001 (Information Security Standard), with 24/7/365 onsite monitoring and security, state-of-the-art fire detection and suppression systems. Redundant power distribution units and diesel generators.

Security

- Access to the datacentre is controlled by security guards.

- Military level 256-bit AES Encryption.

- Access to the data suite is allowed only to authorised staff, their guests and authorised customers. This is enforced via a swipe card system.

- All entrances and exits to the building are monitored by CCTV.

- Access to servers is behind number of security controlled doors.

Connectivity & Power

- Highly resilient MESH network of tier 1 providers with a 100% SLA on internet connectivity.

- Provided by on-site dedicated ESB substations.

- Backup 10,000 litre diesel tank and generator, multiple Uninterruptible Power Supply (UPS) units with transformers as well as 10 tonnes of batteries.

The data centre buildings are typically designed with four layers of physical security;

1. The perimeter fence
2. The entrance
3. Access systems into the rooms
4. Secure, locked cabinets

Extra levels can be introduced such as lockable cages or cubes (containment aisles). No-one enters or leaves without proof of identity, and all visitors are checked against customer-defined access lists. All building areas are secured by an alarm system, and an external security firm patrols the area, both inside and outside.

- Multiple physical security layers, including CCTV, zoned access control

- 24x7 controlled access

Controlled Environment

For optimum performance, all equipment is maintained and continuously monitored in a climate-controlled environment. The average temperature inside the cold aisle is controlled between 18 and 25°C and a humidity level of 50% ± 10%. Multiple air conditioning units provide redundant capacity. Fire-retardant walls, early warning laser smoke detectors (underneath and above the flooring), direct lines to fire stations, and automatic gas-based fire suppression systems provide world-class protection against fire.

- FM200 gas fire suppression system
- SLAs on temperature in line with ASHRAE recommendations
- Entire facility infrastructure monitored 24x7 (CRAC, Fire Panels, Generator, UPS etc.) by Building Management

Access Code Administration of Data Centre

A Security Control Module (stand-alone software) controls the functionality of access security codes and door lock settings to the secure Data Centre. The Data Centre Technical Director reviews an on-line report from the Security Control Module of any access attempts to unauthorized locations weekly Access is restricted to the Security Control Module; the user must have access to the system where the module resides and secondly, the user must have module access. Only two people have this access: Data Centre Technical Director and Senior Network Engineer.

They each have their own username and password for Security Control Module access.

For access to the system where the module resides, a system-based control is in place that requires users to change their password every 90 days. In the case of a server failure or other event where the Security Control Module goes down, the security settings of the Security Control Module will still be intact.

For access security code requests (new requests, changes, suspensions, and terminations), notification of the request is reported to Human Resources and Human Resources submits the request (via email) to the Data Centre Technical Director. The Data Centre Technical Director reviews each request and works with the appropriate manager if there are any questions regarding the request. The Technical Director maintains a hard copy of the email that shows request / approval of access card activity. The Technical Director performs a semi-annual review of access code rights for all NOC

How We Secure Our Networks

We use the same world-class security as global banks do for their banking. For example, we encrypt all data transmissions that involve our systems using SSL 3.0 certificates from GeoTrust to ensure that prying eyes cannot use data that might be intercepted. We employ managed firewalls at datacentre level and use internal protocols to segregate traffic between the application and database tiers.

How We Safeguard Your Data

epicCare uses a layered approach to protect your data from simple storage device errors, catastrophic failures, and everything in between. To support basic database recovery scenarios, we back up all of your data on a rotating schedule of incremental and full backups that let us restore service more efficiently should the need arise.

We utilise a monitored back up service provided by KeepItSafe. This service is provided to ISO 27001. To maintain this elite certification, regular audits are conducted by KeepItSafe to ensure continued compliance and your ongoing data protection.

Once your data is transported off-site via the Internet, they're stored in multiple, independent, and geographically distinct data centres, with 24/7 on-site monitoring to guarantee continuous service even if one data centre fails. This service runs identical, high-redundancy, enterprise-class infrastructure in all data-centre locations, with power, storage, and connectivity all set up to provide high availability.

KeepItSafe's backup solution includes:

- 24/7 data centre security and state-of-the-art fire detection and suppression systems.

- Military-level, 256-bit AES software encryption, which ensures that data remain encrypted both in transit and at rest.
- In-file delta technology certifies that only changes in large files are ever backed up, ensuring lightning-fast backups and resource usage.
- A snapshot/rollback feature allows rollback to file versions as they existed at a given point in time.
-

  Registered with the IE Data Protection Commission.
- Guaranteed Connectivity - Highly resilient MESH network of Tier 1 providers provides KeepItSafe with a 99.9% SLA on Internet connectivity.
- Extremely Secure - Controlled access, 24/7 security guards, swipe-card identification system, CCTV monitoring.
- Guaranteed Power - Dedicated, onsite ESB substations, backup generator, multiple UPS units with transformers along with 10 tonnes of batteries.
- Active VESDA fire-detection system and a passive fire-detection system.

How We Secure epicCare Database

epicCare's database is the underlying data persistence technology at the heart of most cloud services, so it implicitly plays a significant role in the security of the applications that use it, including:

- Custom built client specific database instances
- Our own line of database access protocols
- Server and port access protocols

epicCare has many features that help provide a secure environment and protect the privacy of your business data. One simple example is the way that epicCare protects user passwords with 128-bit cryptographic hash function and IP association.

epicCare's innovative multitenant database architecture delivers automatic scalability for cloud-based applications without compromising the security of each organization's data.

When a user establishes a connection, epicCare utilises session management to put access in context of an organisation.

epicCare confirms that the user context (an organization ID) accompanies each request and includes it where all SQL statements are executed to ensure the request targets the correct organization's data. Data is recorded as a contemporaneous record of that access context, linked to the user log in.

We also use additional validation checks to ensure that accidental or intentional accessing other customers' data is virtually impossible.

How You Can Control System Access

epicCare has a full complement of features for managing users, authenticating and restricting their system access, and curtailing access. You, the customer, retain complete control over who has access and are encouraged to integrate into your existing on-premises access management systems and policies to ensure the highest degree of accuracy, efficiency, and accountability.

How You Can Control Data Access

You can use several epicCare features to control screens, modules, and specific data records to which your users have access. Here's a preview of how it's done.

- **Create profiles and permission sets** – Identify the different types of users you need for your application, based on the different functions each type needs to access. Permissions can be deployed on an individual user basis.

- **Assign users** – Assign each user to the appropriate profile and permission set, such as the areas or modules they work in.
- **Set sharing models** – Data in specific areas can be shared among specific users or areas of an organisation based on how clients have their application configured.

How You Can Audit Data Modifications

All records in the epicCare system are time-stamped and associated with user input. All logins to the application are logged along with IP addresses used. There are a number of reports to show who modified records, version of records prior to modification and audit trail of changes.

Summary

epicCare is committed to building and sustaining your trust as a cloud computing provider. We certify our data centres and our internal operations to some of the highest industry-accepted standards for data security, privacy controls, and operational use. We also offer you specific epicCare features that you can use to deploy applications that secure your data.