guardianERM.net

Security & Disaster Recovery Summary

Overview

We recognize that information security practices are important to our clients.

Just like all information technology, the GuardianERM system is inherently exposed to risks. InConsult recognises these risks and has developed a range of control and recovery measures to ensure confidentiality, integrity and availability.

Application Security

GuardianERM allows each client to control who has read and/or write access to which modules and business units. Clients are responsible for user access rights within their database.

Strong password security is an important first step in protecting GuardianERM user accounts.

GuardianERM allows each organisation to customise system password rules to conform to its own internal security policy. Each client can set password expiration periods, password length and password complexity.

All passwords are encrypted, salted one-way hashed for maximum security.

Users sometimes leave their computers unattended or they don't log off. To protect against unauthorized access, GuardianERM automatically closes sessions when there is no session activity for a period of time. The default timeout is 1 hour.

End-to-end Encryption

GuardianERM ensures that your data is protected in-transit from your browser to our servers using the strongest Internet encryption technologies.

When your data is stored on our servers it is encrypted-at-rest for further security. This applies to all copies of your data: live, backup and mirrored.

Server Security

GuardianERM production servers are hosted in Sydney, Australia on Microsoft's industry leading Azure platform. Azure offers a broad set of key global and industry-specific standards and supporting materials for key regulations, including ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, and SOC 1, 2, and 3 Reports.

Azure also meets regional and national standards that include - Australia IRAP, UK G-Cloud, the EU Model Clauses, EU-U.S. Privacy Shield, Singapore MTCS, the CS Mark in Japan and Singapore MTCS.

Azure is an Australian Signals Directorate (ASD) Certified Cloud Service provider.

Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence of Azure to the strict security controls these standards mandate.

When data deletion is requested, we use Azure's best practice procedures and a wiping solution that is NIST 800-88 compliant, so your data cannot be accidentally available to a third party.

Our security hardened servers have been locked down to comply with industry best practices. These policies/standards/measures include:

- VPN network protection, Just-in-time access and multi-factor authentication to ensure only InConsult staff access the server.
- Tough firewall and system rules to prevent many types of breaches and restrict access if breached.
- IP address controlled access within the GuardianERM infrastructure.
- Security focussed logging and system auditing to prevent and track cyber attacks.
- Automated security policy monitoring to ensure that our infrastructure always complies with best practises.
- Compliance with a number of security standards including Azure CIS 1.1.0, ISO 27001, SOC TSP. Our compliance across these standards currently sits at 97% and reviewed monthly.

guardianERM.net

Security & Disaster Recovery Summary

Penetration Testing

Azure servers are subject to penetration testing based on seven (7) attack vectors that potentially impact degradation of system integrity, confidentiality and availability.

In addition, InConsult performs periodic penetration tests and cyber security scans to identify potential vulnerabilities.

Data Centre Security

For production and back-up, we utilise world-class data centres in Australia. Access is physically secured at the boundary via Perimeter fence and gate and Mantrap. Human security includes 24x7 security officers, CCTV, recorders, motion detection and Biometric Readers within the building and on the data centre floor.

UPS redundancy is in place and back-up power is provided via 3 x 3,000kVA diesel generators

Application Change Management

Access to GuardianERM is restricted to the InConsult development team for updates, enhancements and maintenance.

All clients are notified of major changes and any planned outages due to upgrades.

Release notes are documented after release of a new version.

System Availability, Backup & Recovery

The GuardianERM platform is designed to provide reliable and continuous availability.

GuardianERM availability is achieved in numerous ways:

- The server is locally protected by Azure Live Migration, which predicts/detects hardware/network failures and moves the entire service to a new physical server without data loss.
- In the catastrophic event that entire Sydney data centre going offline, GuardianERM is protected by a failover in Melbourne, which can be quickly activated using a mirrored snapshot of the server within the 5 minutes prior to the outage occurring.
- All data is backed-up every day and stored externally. We can request a rollback to any of the previous 30 days.

InConsult has a business continuity plan that covers all services including GuardianERM.

The plan is reviewed annually and updated as required.

Component tests of the various disruption scenario's are tested periodically.

Security Monitoring

Every day, new security issues and attack vectors are created. We strives to stay on top of the latest security developments both internally and by working with external security experts.

If you believe your account has been compromised or you are seeing suspicious activity on your account please email us at support@inconsult.com.au

Data Breach

In the event of a data breach, we will promptly notify our clients.

To date, there has been no loss of data, no security breaches and no unexpected service interruptions reported.

Summary date: June 2019