CABOOBLE SECURITY

Your security comes first in everything we do.

If your data is not secure, it is not private. In today's security-conscious world, our goal is protection of your data and credentials.

Cabooble protects the information assets and personal data of our clients. Cabooble are committed to continually improving the security of your personal information and protecting you against various forms of information piracy such as spoofing and phishing. Cloud computing has revolutionized the way organizations manage their business and data, but it has also brought a unique set of security concerns. While some businesses are quick to embrace the agility and convenience of the cloud, others remain hesitant because of fear about data breaches and cybercrime.

Cabooble is have been developed on the Oracle Platform to give you peace of mind. Oracle meets international standards to ensure the security of your data.

Encryption keeps your data private while in transit.

Encryption brings a higher level of security and privacy to our services. When you do things like send an email, share a video, visit a website, or store your photos, the data you create remains in our data centres. Cabooble protect this data with multiple layers of security, including leading encryption technology like HTTPS and Transport Layer Security. Cabooble continuously monitor our services and underlying infrastructure to protect them from threats, including spam, malware, viruses, and other forms of malicious code.

Cabooble never give "backdoor" access to your data or our servers that store your data, period. That means no government entity, has direct access to our users' information. There are times when Cabooble receives requests for user data from law enforcement agencies or court. In those instance our legal team reviews these requests will not permit any access to your profile or data. Cabooble have worked hard to be open about these data requests in our Transparency Report.

Cabooble employs numerous methods to secure your password. We also provide numerous methods to log in to your profile. Remember to use the additional alternatives to log in to your profile. Keep your password secure.

A WORD FROM ORACLE

https://cloud.oracle.com/saas_compliance

ISO 27001:2013 is an international standard that covers the planning, implementation, monitoring, and improvement of an Information Security Management System. This widely adopted global security standard sets out requirements and best practices for a systematic approach to managing company and customer information based on periodic security risk assessments.

Oracle has achieved ISO/IEC 27001:2013 certification for the following SaaS solutions: Taleo Business Edition, Taleo Social Sourcing, Fusion, GNC (SaaS), Responsys, Eloqua, OFSC, and RightNow.

SaaS for OPC and OMCS have been successfully audited against American Institute of Certified Public Accountants (AICPA) Service Organization Controls Type 1 and Type 2 standards for design and operational security. These SOC1/SOC2 audits are refreshed and repeated every 6-months.

Oracle Fusion SaaS for OPC successfully completed independent Health Insurance Portability and Accountability Act (HIPAA)/ Health Information Technology for Economic and Clinical Health (HITECH) Act attestation in January 2017 to add to already attested Fusion SaaS HIPAA deployments in OMCS and On-Premise. Fusion joins other SaaS offerings such as RightNow and Eloqua as being compliant with HIPAA, which regulates patient Protected Health Information in the US.

Oracle offers all HIPAA customers a Business Associate Agreement as part of the contract process which defines each party's responsibilities in protecting all Personal Health Information (PHI) in accordance with HIPAA/HITECH.

The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government-wide program that provides a standard approach to the security assessment, authorization and continuous monitoring for cloud products and services. U.S. Federal agencies are directed by the Office of Management and Budget (OMB) to leverage FedRAMP to ensure security is in place when accessing cloud products and services.

FedRAMP uses the NIST Special Publication 800-53, which provides a catalogue of security controls for all U.S. Federal information systems. FedRAMP requires cloud service providers (CSP) to receive an independent security review performed by a third party assessment organization (3PAO) to ensure authorizations are compliant with the Federal Information Security Management Act (FISMA).

Oracle has achieved FedRAMP authorization for both Oracle Service Cloud and Oracle Government Cloud – Common Controls, and has achieved FedRAMP Ready Status for Oracle Fusion ERP/HCM/CRM Cloud. Additionally, Oracle Planning and Budgeting Cloud Service and Oracle Taleo Enterprise/Learn/Social Sourcing Cloud are each currently under Agency review for a FedRAMP Authority to Operate (ATO).

19 October 2017, 10 January 2018. Last updated 5 February 2018