SECURITY STATEMENT

Bizztracker, legally represented by Limino BV (hereinafter referred to as "Bizztracker") has created this Security Policy in order to demonstrate our firm commitment to security. The following discloses our security and accessibility policies.

Site certificate information

Bizztracker understands that the security of your personal information and business details is important to you. Whenever you submit personally identifiable or business identifiable information or transfer other information and documents to and from bizztracker.com, you will be doing so through secure servers.

The bizztracker.com service only allows secure browsers access to the system. The browser's "secure mode" is in place only when you are logged in to the system. You will be able to tell that you are in a secure mode when your browser displays a special icon on the lower bar of your browser window. Every secure page (i.e. every part of the user interface) on bizztracker.com has been secured with a digital certificate. This is shown via the “site certificate” that is resident on all secure pages. To view this certificate, click on the image of the closed lock on the bottom bar of your browser window. A small frame displaying site security information will appear. This allows you to verify the site certification authority and that you are in fact on bizztracker.com or a sub-domain of bizztracker.com, e.g. app.bizztracker.com.

User identification

Only the members of a community in Bizztracker can see the community and access its contents. Each user selects his/her own password for bizztracker.com. The users’ passwords are stored in a one-way encrypted format and are not accessible to employees of Bizztracker. After entering the required registration information as a new user you will be able to access your user account immediately. The password is chosen directly as part of the registration process and not sent to you by any other means. If you have forgotten your password, or your password is not working for some reason, you can re-establish your identity with the system as follows:

- Go to app.bizztracker.com
- Follow the instructions shown under “Forget your password?”
- An email message will be sent to you with instructions to reset your password.

A password system has been established to ensure that only you can access your personal information and communities. The acceptable minimum password length is 6 characters. We recommend that you use a random combination of letters, numbers, and cases to provide added protection (for instance: 'Hfg358mz' would be a good password).

Each time you login to the system you will be required to authenticate your identity by entering your previously supplied e-mail address and password. Upon successful login, you are issued a unique "session id" (does not include any personally identifiable information) which allows you to remain active as long as actions are performed in the system. In case the session has timed out, it is required to re-enter your e-mail address and password. If an incorrect password is supplied, or if you simply forget your password, you may need to re-establish your identity following the instructions above. After an undisclosed number of unsuccessful login attempts, you will be locked out.

Protection of information being transmitted

We use encryption technology to ensure the safe transmission of your information and documents when logged into the system. Your browser provides security by allowing us to use Secure Socket Layer (SSL) encryption up to 128-bit key length encryption when transmitting information and documents. The number of bits of secret key length varies between 40 and 128 depending on your browser's capability. The highest available bit length is always used. All communication between your computer and app.bizztracker.com is encrypted using SSL.

Protection of stored information

Platform

Bizztracker uses the AWS platform to operate the bizztracker application. AWS is a cloud application platform used by organizations of all sizes to deploy and operate applications throughout the world. This platform allows organizations to focus on application development and business strategy while AWS focuses on infrastructure management, scaling, and security. AWS applies security best practices and manages platform security so customers can focus on their business. The AWS platform inherently protects customers from threats by applying security controls at every layer from physical to application, isolating customer applications and data, and with its ability to rapidly deploy security updates without customer interaction or service interruption.
For detailed information about the security policy of AWS see: https://aws.amazon.com/security

Physical security

AWS's physical infrastructure is hosted and managed within Amazon's secure data centers. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

Amazon has many years of experience in designing, constructing, and operating large-scale

data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
Amazon only provides data center access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centers by Amazon employees is logged and audited routinely. For additional information see: https://aws.amazon.com/security

Employee policy

Bizztracker takes many measures to protect client information while it is stored. Bizztracker has taken special steps to ensure that only a few key people are aware of how the security system is designed and implemented. All employees at Bizztracker are bound by a confidentiality and non-disclosure agreement prohibiting access to and dissemination of information

Privacy

In addition to client data, some personal information is stored in our databases and in browser cookies. For a complete list of what personal and demographic information is stored at Bizztracker.com we refer to our Privacy Statement.

Data Security

Application

The bizztracker application runs within its own isolated environment at the AWS platform and cannot interact with other applications or areas of the system. This restrictive operating environment is designed to prevent security and stability issues. These self-contained environments isolate processes, memory, and the file system using LXC while host-based firewalls restrict applications from establishing local network connections. For additional technical information see: https://aws.amazon.com/security

Data in Oracle Database

The data in bizztracker is stored in Oracle databases. It is stored in a separate access-controlled database. Each database requires a unique username and password that is only valid for that specific database and is unique to bizztracker. The connection between bizztracker and the databases require SSL encryption to ensure a high level of security and privacy.

Back-up

Every change to your data is written to write-ahead logs, which are shipped to multi-datacenter, high-durability storage. In the unlikely event of unrecoverable hardware failure, these logs can be automatically 'replayed' to recover the database to within seconds of its last known state. Bizztracker stores the last 7 day back-ups and 5 week back-ups.

Version 2.0, June 1, 2018