

Data Security Statement

Your data is important and needs to be securely stored and backed up. Ecounting uses the following data security, storage and back up procedure.

1. SECURITY

Access to the **Ecounting** web portal is username and password protected. Data sent between your browser and the server is also secured using a SSL (Secure Socket Layer) certificate just like online banking services to encrypt the information passing between your browser and the server to stop any potential hackers from accessing your data in transit. Once logged into the system, the user can only access information that they have permission to view.

Firewalls are managed by security specialists and deployed in a private IP space, while servers and routers are segregated in Virtual Local Area Networks (VLAN). Network security features also include multi-level privileges, OS lock downs and monitored change logs.

Our server manager is constantly engaged in threat analysis seeking to identify and address security weaknesses in servers, applications and activities.

Security patching is performed by constantly updating our security systems. Monitoring and addressing emerging threats, and quickly processing and applying new security patches is standard procedure. This ensures optimum protection for your data.

2. WORLD CLASS DATA STORAGE & NETWORK OPERATIONS

Our data storage facility is a tier-1 facility in shared commercial space. For security reasons the location of the facilities is not disclosed. The facility is owned by a large multi-national corporate and is an ultra-high security, highly redundant, purpose-built facility.

The facility operates 24 hours a day, 365 days a year. It has the highest levels of redundancy in its region, automatic fail-over capability and capacity to cater for rapid growth in demand.

3. BACKUPS

Ecounting uses a resilient backup process including redundant backups to both disk and tape.

FIRST LEVEL PROTECTION – RESILIENT MASS DATA STORAGE

Ecounting is a dynamic system that uses a relational database server to store your data. To reduce the risk of data loss and to ensure storage capacity remains adequate, RAID storage arrays are used.

Ecounting

These storage systems accommodate multiple hard disks and are fault tolerant. In the event of a single hard disk failure, the system will keep working with no data loss. The hard disks can be “hot-swapped” meaning that a technician can replace a faulty drive while the storage system is still working without data loss.

SECOND LEVEL PROTECTION – DAILY BACKUP

An automatic backup process using tape is run on a daily basis. The tape are rotated off site to storage vaults on a weekly basis. This provides added security for your data. For redundancy and speed in recovery, backups are also written to a disk image.

THIRD LEVEL PROTECTION – WEEKLY BACKUP

Your data is backed-up each week at a completely different site. This is done to further protect your data in the extremely unlikely event that our servers and backups are lost due to disaster. Note that, in the event of a hard disk failure, the system will keep working with no data loss.

As mentioned above, should there be the need to replace a hard disk, they can be “hot-swapped” meaning that a technician can replace a faulty drive while the storage system is still working without data loss.