Access and Security

July 2015

Your data is safe with webCRM.
In fact far safer than most in-house applications

webCRM access

- Up to 90 security access levels.
- Grouping of users with similar rights.
- Restrict access to records by Territories and Responsible.
- Restrict Access to View, edit or delete.
- Restrict Access to menus, modules and Utilities.
- Restrict Access by Report and data exporting.
- IP addresses are logged.
- Separate and private database for each customer.
- More that 3 faulty login attempt causes user to be blocked.

Infra structure

The webCRM servers are held in highly secure, under-ground purpose built facilities, and are managed around the clock. Our servers are always kept updated with the latest security patches.

- 24/365 SLA Access at 99.97% up-time.
- Powerful Cisco routers.
- Two hardware based stateful-inspection firewalls.
- 2 central layer3 switches.
- Two redundant Gbyte fibre Internet connections.
- Redundant power supplies and fire protection.
- A 160KW diesel generator stands by in case of a power cut.
- Data is stored using raid disk technology.
- Daily back-up to a secondary location.
- Https secure socket layer for data encryption.

Procedures and Certifications

webCRM is hosted at Dandomain in Denmark. A leading and proven hosting provider.

http://www.dandomain.dk

Dandomain handles security including server access, patches and updates applying best efforts to install such patches and updates.

Dandomain is PCI certified (Credit Card Information) and ISAE 3402 certified and webCRM is satisfied that Dandomain apply same procedures and practice for Credit Card Information servers as for the webCRM servers as far as the physical security is concerned.

All webCRM servers are behind a statefull firewall and monitored by an IDS (intrusion detection system). Additionally 2 private networks for AD authentication and iSCSI (Internet Protocol for storage networking).

Each webCRM customer has his own MS SQL database (physical file) with a unique random name. On-line incremental backup at hourly interval and a full backup every 24 to a separate location hours is applied

From the webCRM Configuration menu the customer can permit or deny webCRM support staff to log in to the customer system in order to handle support tasks. In case the customer has denied webCRM support staff to log in to his webCRM system only one trusted individual from webCRM can force a re-open of the support access and will do so only upon the customer’s request.