VERICO

Microsoft
Dynamics CRM

Verico Dynamics

Table of Contents

VERICO DYNAMICS SECURITY OVERVIEW

VERICO Dynamics utilizes some of the most advanced technology for Software Systems and Internet security available today. System and Data security and protection is our primary concern and was a key consideration in our selection of suppliers such Microsoft, Click Dimensions and Rackforce Networks.

When you access Verico Dynamics you are using industry standard Secure Socket Layer (SSL) technology, your information is protected using both server authentication and data encryption, ensuring that your data is as safe, secure, protected as possible in compliance with the latest commercially reasonable standards. VERICO Dynamics provides each registered User in your organization with a unique user name and password that must be entered each time a User logs on to the system. It is your responsibility and also a condition of system use to protect your data and passwords. User access is restricted to registered and authorized Users of the system through Microsoft role based security and authentication. For more information please read the Microsoft Security document located here.
http://www.vericodynamics.ca/docs/CRM4_NB_SEC_PT1_Architecture1_1.pdf

In addition, VERICO Dynamics is hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders. To report security issues to VERICO Dynamics please contact us immediately at dynamics@verico.ca

MICROSOFT TECHNOLOGY

The VERICO Dynamics system is based on a combination of enterprise class software provided by Microsoft. The software platform includes

1. Microsoft SQL Server
2. Microsoft CRM Dynamics
3. Microsoft SharePoint
4. Microsoft Forefront

In addition, these Microsoft technologies integrate with Microsoft Office products such as Outlook and Internet Explorer.

MICROSOFT SOFTWARE LICENSING

The software is used under a group Service Provider License Agreement between Microsoft Canada and Verico Financial Group Inc. Each user of the software must purchase a Client Access License (CAL) from Microsoft Canada through the system in accordance with all Microsoft CAL terms and conditions and the VERICO Dynamics End User License Agreement (EULA). https://register.vericodynamics.ca/ As a registered user you must agree to and accept the terms of service and use contained in this EULA which limits the liability of Microsoft and VERICO.

DATA CENTRE SECURITY

The Microsoft Software System is hosted by Rackforce Networks. RackForce Networks is a privately held ICT service provider based in Kelowna B.C., Canada. Founded in 2001. RackForce supports thousands of customers from over 100 countries.

Certifications

Among other important and industry recognized certifications that RackForce and its employees have earned, the following key certifications allow you to feel even more confident that outsourcing and out-tasking to RackForce is the best choice for your ICT requirements.

CICA 5970 Type B Certification

CICA 5970 is a Canadian standard administered by the Canadian Institute of Chartered Accountants. Designation under this program encompasses specific requirements for service providers managing customer data and focuses heavily in the areas of compliance, security and access. In addition, this certification addresses the topics of backup and recovery, computer operations and facility infrastructure.

SAS 70 Type II Certification

The SAS 70 is issued by the Auditing Standards Board of the American Institute of Certified Public Accountants to service organizations that typically offer outsourced services. An auditor's report details the ability for a service provider's ability to offer adequate controls and safeguards when they host or process data belonging to their customers.

RACKFORCE BACKGROUNDER

RackForce's roots are based in Internet infrastructure hosting where they have earned a reputation for leadership and innovation. RackForce has consistently provided market leading services by selectively leveraging emerging technologies to provide cost effective, innovative offerings.

In the 2005-2007 period RackForce developed strategic relationships with major technology leaders, such as Microsoft, IBM and Cisco Systems. This enables RackForce to have early access to game changing intelligence, products and technologies. RackForce translated these advantages into the development of new enterprise-class services, revising its capabilities to focus more directly on the enterprise market.

Today its services are represented in its ‘4 Pillars’ infrastructure services portfolio. They focus totally on infrastructure services - up to, and including the Operating System layer. RackForce's mission is to provide industry leading services that enable organizations to buy infrastructure-as-a-Service (IaaS) solutions, in a cost effective and flexible model, leveraging to as large an extent as practical, the latest technologies and innovations. They deliver these services from its new class-leading ‘GigaCenter’ data center in Kelowna, as well as our secondary Kelowna facility and a Toronto facility.

RackForce’s 4 Pillars services portfolio consists of:

- Colocation Services
- Servers Services, including dedicated, virtual and Cloud services
- Network Services
- Managed Services and Disaster Recovery Services

RackForce takes a holistic approach to delivering its services in a most secure manner. They understand protecting client data and privacy is job one. The primary elements that comprise its security programs include:

- Physical Security - focused on the facility
- Security Processes - largely the people aspects of our security programs
- Network Security - protecting the transport of data
- Security of Cloud Services - ensuring our hosted private Cloud services are delivered with confidence

Physical Security

The ‘GigaCenter’ data center employs multiple mantrap security measures - proximity pass, fingerprint, and security code. There are seven layers of security between the front door and an individual computer rack. Physical security measures include:

- Security Cameras throughout the facility
- Multiple pan-tilt-zone cameras outside the facility
- Cameras images are recorded, searchable and archived for a minimum of 90 days
- Proximity pass and biometric scanners at multiple access points
- Motion sensors and intrusion detection sensors
- Audible alarm system is sounded immediately upon the triggering of any sensor
- Steel doors and two-stage man traps
- Computer racks are individually locked
- Access control system is located in a locked cabinet in a secure room that's only accessible by authorized personnel
- Manned and monitored security desk
- Security systems are monitored 7x24 by both the on-site NOC and an off-site third party

Security Processes

RackForce employees extensive security processes that support our clients' needs. Our processes have been audited by a third party by evidence of our SAS70 certification. Further information can be obtained by contacting our Chief Security Officer, Randall Robinson.

Existing, audited processes include:

- All entrances are locked at all times; Two factor authentication (badge and biometric) is required for access to the facility and to the data halls
- All employees and authorized (badged) contractors are subject to a criminal record check
- All employees must wear a photo-ID badge at all times while in the facility
- Each employee and authorized contractor must use their access badge in when arriving, and badge out when leaving the facility (no tailgating); a perpetual log is maintained of what personnel are onsite
- Badge and biometric access is controlled in zones, ensuring personal have access to authorized areas only
- Changes to access are documented and approved by management
- The ability to create, modify or delete access authorization is restricted by management
- Processes are in place to remove access when an employee or contractor is terminator or a badge is lost
- The access control system is logged, searchable and archived; logs are retained for at least 90 days
- Visitors are required to sign a visitor log, provide a government issued photo ID, and wear a visitor badge while in the facility
- Visitors are escorted at all times
- RackForce personnel are on-site 7x24x365.

The RackForce Chief Security Officer is responsible for the ongoing review, management, optimizing and documenting the Security Plan.

Network Security

The GigaCenter is carrier-neutral and is served by numerous major Canadian telcos, including Shaw, Bell, Rogers, Allstream and Telus. RackForce also manages a private 10Gbps network into major Canadian cities, including Vancouver, Calgary and Toronto, and Seattle Washington. This provides access to high capacity, low cost bandwidth from major North American and International communications providers. Data on the RackForce private network is transported at layer 2. RackForce can cross connect with the client's preferred telco at the peering points mentioned above, providing a secure and highly available service.

Clients can procure network services directly from their preferred telco, or purchase network services from RackForce and our telco partners. Clients can use their own VPN and encryption technologies to support their security requirements, for services delivered from the GigaCenter.

Fiber feeds into the GigaCenter are delivered through diverse underground conduits into the facility.

The data center LAN is fully redundant with 10Gbps capability to every cabinet and device within the facility. Built on the Cisco Nexus 3.0 platform, it has no single points of failure and supports concurrent maintenance. All customer data traffic is isolated on private VLANs within our GigaCenter switching with separate layer 3 routing interfaces created per VLAN at the core routing layer. No layer 2 traffic is carried between VLANs, and logical layer 2 VLAN segments are never shared between clients.

A number of optional and highly recommended services are available to enhance our clients' security programs:

- Firewall & Network Security Gateway
- Includes IPS and IDS
- Includes customer portal for self management and customization
- Web Security service
- Web Application Security service
- Email Security service

Security of Cloud Services

A key element of our Cloud security is the separation of client's data traffic at layer 2, on both the RackForce private WAN and GigaCenter LAN. Each client has their own private VLAN, and VLAN segments are not shared between clients.

Other aspects of our Cloud security include:

- Each Cloud VM has its own dedicated server RAM
- Each Cloud VM has its own dedicated SAN space - SAN space is allocated privately in a secure multi-tenant model
- Virtualization is delivered using industry leading VMware vSphere
- Cloud server infrastructure is delivered from a RackForce owned and managed high security vault within the GigaCenter facility.

IBM TIVOLI

IBM

Tivoli software

Enterprise Backup & Failover Systems

RackForce provides data backup services utilizing IBM's Tivoli Storage Manager (TSM). RackForce's TSM backup solution includes both onsite and offsite[1] electronic vaulting in a single enterprise class backup package.

Utilizing TSM's Smart Data Store technology, RackForce's backup solution backs up your defined data nightly to a storage pool at the primary onsite location, and then moves the data to a second storage device in a secure offsite[1] location within the following 24 to 48 hours. The most recent "active" copy of each file is retained at the onsite location to facilitate faster restore times while offsite copies ensure resiliency and security for backed up data.

TSM is fully automated and its centralized policy management system allows authorized VERICO Dynamics Systems Administrators to dictate which files are included or excluded from backups. Generally we have backed up all data in the SQL Database.

How It Works:

- RackForce has installed TSM client(s) as required on our server(s) that gives the system control over what files are included or excluded
- Your data is first backed up to hard disk (SAN or NAS) in the primary onsite facility.
- At regular intervals your onsite stored data is copied to a secure offsite[1] storage pool.
- RackForce uses a centralized TSM server to control your backups.
- The Dynamics system has full control of restores from the TSM client installed on your server(s)
- Alternatively authorized Systems Admin may request assistance through a support ticket opened from inside the Rackforce Customer Service Center portal.

HUMAN ERROR RISK PREVENTION

As reported in Computer World magazine, Uptime Institute, a research and consulting organization, evaluated 4,500 incidents affecting data centers and found that approximately 70 percent of the reported problems were not caused by a default in the technology but instead caused by human mistake.

Similarly many privacy breaches and security risks at the user level are the result of human oversight and error. It is important to follow generally accepted best practices in the management of your Verico Dynamics user account.

VERICO DYNAMICS PASSWORDS

- VERICO Dynamics Passwords should be treated as confidential information. No employee Broker or Agent is to give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends, or family members, under any circumstances.
- If someone demands your password, refer him or her to these guidelines or have him or her contact your IT Department.
- Passwords should not be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to company resources via the company's IPsec-secured Virtual Private Network or SSL-protected Web site such as VERICO Dynamics.
- No employee, Broker or Agent is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access place if in hardcopy form or in an encrypted file if in electronic form.
- Do not use the "Remember Password" feature of applications and do not create a "hot key" for password use.
- Passwords used to gain access to Verico Dynamics systems should not be used as passwords to access non-Verico Dynamics accounts or information.
- If possible, don't use the same password to access multiple VERICO systems.
- If an employee, Broker or Agent either knows or suspects that his/her password has been compromised, it must be reported to the VERICO IT Department and the password changed immediately.
- Finally, please remember that there is no need to share IDs and passwords. Anyone who needs and qualifies for access to the VERICO Dynamics system should submit a request for his or her own LogonID and password through the appropriate registration page.

PERSONAL COMPUTER PASSWORD

Your computer password is your personal key to your computer system. Passwords help to ensure that only authorized individuals access your computer system. Passwords also help to determine accountability for all transactions and other changes made to system resources, including your data. If you share your password with a colleague or friend, you may be giving an unauthorized individual access to the VERICO Dynamics system and privacy protected data.

Authentication of individuals as valid users, via the input of a valid password, is required to access any shared computer information system. Each user is accountable for the selection, confidentiality and changing of passwords required for authentication purposes. Since you are responsible for picking your own password, it is important to be able to tell the difference between a good password and a bad one. Bad passwords jeopardize information that they are supposed to protect. Good ones do not.

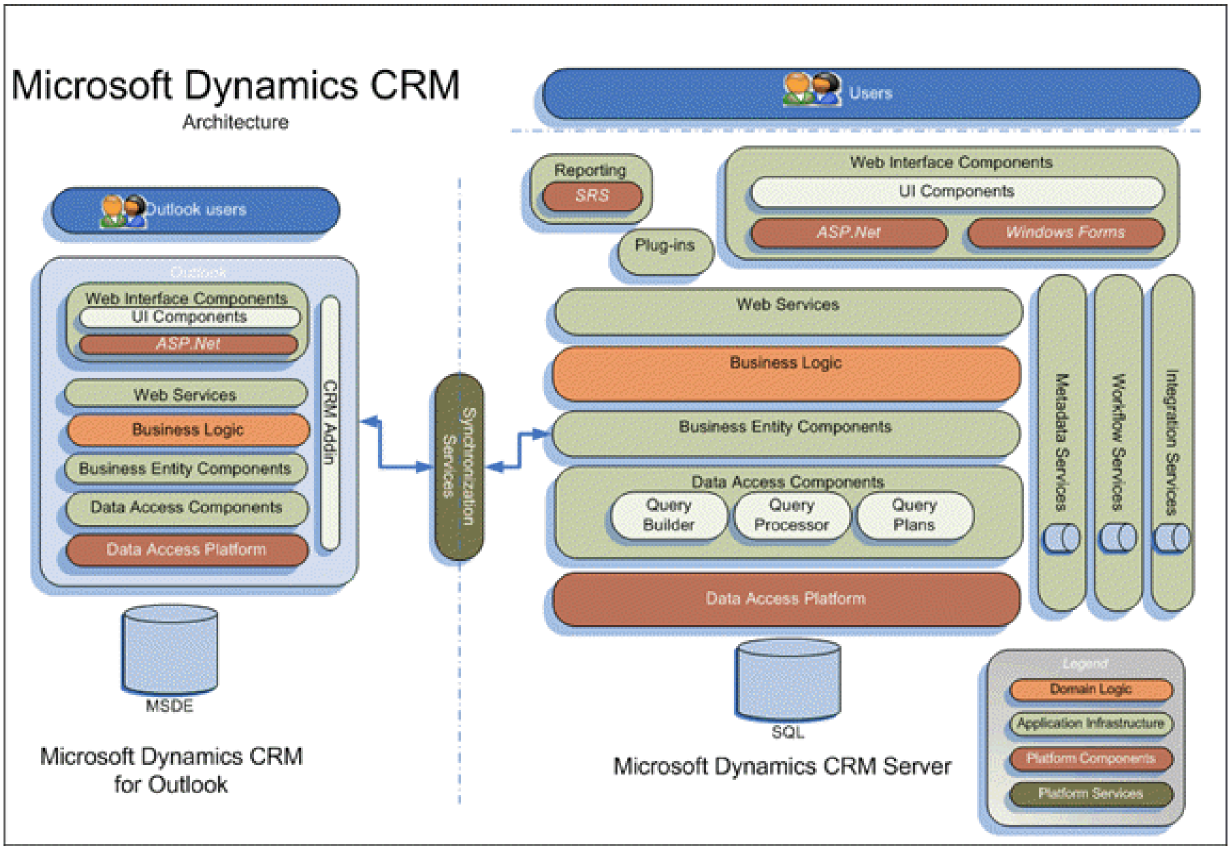
Your password should not be the same as your User/LogonID, an anagram of your User/LogonID or a palindrome of your User/LogonID. If you have access to a number of systems that require the entry of a password, such as the mainframe computer and a Local Area Network (LAN), try not to use the same password for both systems. A good password is relatively easy to remember but hard for somebody else to guess. There are a variety of techniques you can use to choose secure passwords. Listed below are some examples of creating passwords.

- Passwords should be changed every 60 days.
- Old passwords should not be re-used for a period of 6 months.
- All passwords should conform to the guidelines outlined below.

Passwords are used to access any number of systems, including networks, e-mail, the Web, and voicemail. Poor, weak passwords are easily cracked, and put the entire system at risk. Therefore, strong passwords are required. Try to create a password that is also easy to remember.

- Passwords should not be based on well-known or easily accessible personal information.
- Passwords should contain at least 8 characters.
- Passwords should contain at least 5 uppercase letters (e.g. N) or 5 lowercase letters (e.g. t) or a combination of both.
- Passwords should contain at least 2 numerical characters (e.g. 5).
- Passwords should contain at least 1 special characters (e.g. $).
- A new password should contain at least 5 characters that are different than those found in the old password, which it is replacing.
- Passwords should not be based on users' personal information or that of his or her friends, family members, or pets. Personal information includes logon I.D., name, birthday, address, phone number, social security number, or any permutations thereof.
- Passwords should not be words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon.
- Passwords should not be trivial, predictable or obvious.
- Passwords should not be based on publicly known fictional characters from books, films, and so on.
- Passwords should not be based on the company's name or geographic location.

DIAGRAM 1 – MS Dynamics CRM Architecture


Microsoft Dynamics CRM
Architecture
Users
Outlook users
Outlook
Web Interface Components
UI Components
ASP.Net
Web Services
Business Logic
Business Entity Components
Data Access Components
Data Access Platform
CRM Addin
MSDE
Microsoft Dynamics CRM for Outlook
Synchronization Services
Reporting
SRS
Plug-ins
Web Interface Components
UI Components
ASP.Net
Windows Forms
Web Services
Business Logic
Business Entity Components
Data Access Components
Query Builder
Query Processor
Query Plans
Data Access Platform
Metadata Services
Workflow Services
Integration Services
SQL
Microsoft Dynamics CRM Server
Legend
Domain Logic
Application Infrastructure
Platform Components
Platform Services