

Project Hosts Security Assessment

Project Hosts follows the recommended Security Controls of Federal Information Standards in accordance with (NIST) National Institute of Standards and Technology U.S. Department of Commerce

27 July 2007

Control Name	Control
Access Control	
AC-1 Access Control Policy	Policies are in place that control access to the system. Every Customer deployment has a single authorized representative (“Customer rep”). This representative is the only one with authority to grant administrative access to Customer personnel. This grant of access must be done in writing, usually via email, and may include administrative access to applications, or also admin access to OS and databases for Customer-dedicated environments.
AC-2 Account Management	Project Hosts has a system in place that manages and maintains all System Accounts. Project Hosts allows our customer to have administrative access to their own dedicated servers, therefore giving the customer sole discretion on how they manage and maintain their own user accounts.
AC-3 Access Enforcement	Every customer has a single authorized representative. This representative is the only one in authority to grant administrative access to customer personnel. This grant of access must be done in writing, usually via email, and may include access to applications, or also admin access to OS and databases for Customer-dedicated environments.
AC-4 Information Flow Enforcement	All communication between client PCs and the hosted CRM environment is made through SSL. This protocol employs 128-bit encryption to protect data in transport.
AC-5 Separation of Duties	There are various levels of access to different personnel, with only the amount of access needed to perform their required roles. For example, support personnel have administrative access to applications, but not to the OS, database, or domain. Access to a customer’s OS and database are restricted to engineers associated with that customer’s deployment. Domain access is restricted to a small group of domain administrators.
AC-6 Least Privilege	There are various levels of access to different personnel with only the amount of access needed to perform their required roles. For example, support personnel have administrative access to applications, but not to the OS, Database or Domain. Access to customers’ OS and databases are restricted to domain administrators.
AC-7 Unsuccessful Login Attempts	Project Hosts allows 5 failed password login attempts before the application locks out the user.
AC-8 System Use Notification	A system use notification message could potentially be posted for non-administrator users accessing the system through their web browser for an additional charge . However, if non-administrator users are only allowed to access the system through their Outlook client, then our understanding is that this requirement will be met by the existing customer client PC security measures.
AC-9 Previous Logon Notification	The system maintains a running log of previous logons along with the date and time of that particular login. But the user does not see the last login notifications. This log is for security record keeping only.
AC-11 Session Lock	No session lock is normally applied. A session lock could be implemented for non-administrator users, if required, for an additional charge . However, if non-administrator users are only allowed to access the system through their Outlook client, then our understanding is that this requirement will be met by the existing customer client PC security measures.
AC-12 Session Termination	No session termination is normally available. A session termination could be implemented for non-administrator web browser users, if required, for an additional charge . However, if non-administrator users are only allowed to access the system through their Outlook client, then our understanding is that this requirement will be met by the existing customer client PC security measures.
AC-13 Supervision and Review – Access Control	Supervision and Review of Access Control happens on a regular basis and is updated as deficiencies or lapses in security are identified.

AC-14 Permitted Actions w/o ID or Auth	There is no system access without login with valid credentials.
AC-15 Automated Marking	Does not apply
AC-16 Automated Labeling	Does not apply
AC-17 Remote Access	<ol style="list-style-type: none"> 1. Project Host has policies in place to help protect against an unauthorized security breach. 2. SSL token cryptography along with username and password is used to prevent against unauthorized access. This sets up a secure end-to-end link over which http or any other application protocol can operate. 3. Only access to an open port is allowed. If a closed port is intruded against, the token or packet is dumped and or rejected.
AC-18 Wireless Access Restrictions	There is no wireless device access to the system except through wireless web access where normal security policies apply.
AC-19 Access Control for portable/mobile systems	There is no portable/mobile system access to the system except through wireless web access where normal security policies apply.
AC-20 Use of External Information Systems	No outsourced information systems, so does not apply.
Awareness and Training	
AT-1 Security Awareness Policy	A Security Awareness Policy is in place and is available to all employees.
AT-2 Security Awareness	Initial training is provided to employees on the responsibilities and application rules as they pertain to the Security Awareness Policy at the beginning of employment. Project Hosts will continue to provide the necessary training on their responsibilities and the application rules as the rules change. Customer security awareness training is typically supplied by an onsite CRM implementation partner.
AT-3 Security Training	Security training is typically supplied by an onsite CRM implementation partner.
AT-4 Security Training Records	Security records are typically maintained by an onsite CRM implementation partner.
AT-5 Contacts with Security Groups and Assoc.	Does not apply
Audit and Accountability	
AU-1 Audit and Accountability Policy	Regular vulnerability assessments and audits on the production and system environments annually by a third party. Customers can also initiate audits of the Application Infrastructure without any restrictions or conditions on an as needed basis.
AU-2 Auditable Events	Audit logs are maintained for application security as well as full Windows system logs.
AU-3 Content of Audit Records	Audit logs are maintained for application security as well as full Windows system logs.
AU-4 Audit Storage Capacity	Adequate audit log storage capacity is available to maintain a record of all important audit events.
AU-5 Response to Audit Processing Failures	All audit processing failures are reported to our Chief Technical Officer (CTO) where they are reviewed and proper adjustments are made to correct the deficiencies as needed.
AU-6 Audit Monitoring, Analysis and Reporting	Security audit logs are reviewed on a periodic basis and exceptions are reported to the designated client contact.
AU-7 Audit Reduction and Reporting	Audit logs are maintained electronically for a period of at least one year.
AU-8 Time Stamps	Audit logs are time stamped with date and time when an issue occurs.
AU-9 Protection of Audit Information	Audit logs are maintained in a secure database.
AU-10 Non-repudiation	
AU-11 Audit Retention	Audit logs are maintained electronically for a period of at least one year.

Certification, Accreditation and Security Assessments	
CA-1 Certification, Accreditation and Assessment Policy	The CRM product selected must follow the customer C&A
CA-2 Security Assessments	Customer Cyber security and OIG staff will periodically audit the application
CA-3 Information System Connections	The system does not connect to other information systems outside of the accreditation boundary.
CA-4 Security Certification	The CRM product falls under the customer C&A
CA-5 Plan of Action and Milestones	When necessary, a plan of action with milestones is developed to resolve identified remedial actions.
CA-6 Security Accreditation	The CRM product falls under the customer C&A
CA-7 Continuous Monitoring	Our Chief Technical Officer (CTO) manages and monitors our Security controls on a regular and continuous basis.
Configuration Management	
CM-1 Configuration Management Policy	The CTO's office maintains standard procedures and policies for system maintenance and management.
CM-2 Baseline Configuration	A system baseline configuration is generated and maintained in the environment build documents.
CM-3 Configuration Change Control	Configuration changes requested by customers are recorded in electronic form in a secure database.
CM-4 Monitoring Configuration Changes	The impact of configuration changes on system security is analyzed prior to change implementation.
CM-5 Access Restrictions for Change	Individual access privileges and physical and logical access restrictions are authorized only upon written customer approval.
CM-6 Configuration Settings	Configuration settings are defined and documented and implemented upon system launch. The customer administrator controls application roles-based security.
CM-7 Least Functionality	The system is only accessible through SSL port 443 and users are limited to essential capabilities.
CM-8 Information System Component Inventory	An inventory of the network components is maintained and updated upon change.
Contingency Planning	
CP-1 Contingency Planning Policy	The CTO's office maintains disaster recovery policy and procedures for timely response to foreseeable contingencies.
CP-2 Contingency Plan	Disaster recovery policy and procedures have been developed for timely response to foreseeable contingencies.
CP-3 Contingency Training	The contingency plan is reviewed periodically and updated training is provided when necessary.
CP-4 Contingency Plan Testing	The contingency plan is tested periodically.
CP-5 Contingency Plan Update	The contingency plan is updated on a regular basis.
CP-6 Alternate Storage Sites	System data is backed up daily and tape backups are stored in a secure, off-site location on a daily basis for 90 days. The system data backup is managed for Project Hosts by Qwest at Qwest's preferred, secure offsite vendor.
CP-7 Alternate Processing Sites	Project Hosts maintains data centers at two physically distinct server hosting sites
CP-8 Telecommunication Services	Qwest is our External Information System services provider for data backup and Internet access. Agreements are in place with Qwest regarding network access, services, and physical and network security policies.
CP-9 Information System Backup	The system is backed up to disc daily on another server. Then the data is backed up to tape. Backup tapes are then copied and moved to an offsite location.
CP-10 Information System Recovery	The defined disaster recovery process defines roles, responsibilities, and procedures for recovering and reconstituting the system data after a disruption or failure.
Identification and Authentication	
IA-1 Identification and	The CTO's office maintains identification and authentication policies and procedures.

Authentication Policy	
IA-2 User Identification and Authentication	Strong password requirements are maintained for all deployments. These passwords that are made up of combinations of upper and lowercase letters, symbols and numbers are extremely effective in preventing unauthorized access. See SA-2 for further explanation.
IA-3 Device Identification and Authentication	Application access via the web service is restricted to the vendor and customer hosts and IP addresses. See boundary protection.
IA-4 Identifier Management	Identifier management is controlled through Active Directory security.
IA-5 Authenticator Management	Authenticator management is handled through Active Directory security.
IA-6 Authenticator Feedback	Active Directory information is encrypted for security.
IA-7 Cryptographic Module Authentication	Active Directory information is encrypted for security.
Incident Response	
IR-1 Incident Response Policy	The CTO's office maintains policies and procedures for incident response.
IR-2 Incident Response Training	Periodic review and training for incident responses.
IR-3 Incident Response Testing	Periodic incident response testing is conducted.
IR-4 Incident Handling	Standard procedures for security incident handling are in place.
IR-5 Incident Monitoring	Continuous monitoring of the system security is tracked and recorded in a secure database.
IR-6 Incident Reporting	Security personnel are notified automatically in the case of a security incident. The customer system administrator would be notified in the event of a security incident.
IR-7 Incident Response Assistance	Incident response support is available on a continuous basis. Coordination with the customer system administrator would be implemented for the duration of any incident response.
Maintenance	
MA-1 System Maintenance Policy	The CTO's office maintains standard procedures for system maintenance.
MA-2 Periodic Maintenance	Periodic maintenance is completed on an as-needed basis.
MA-3 Maintenance Tools	Maintenance tools are approved and maintained on an ongoing basis for use.
MA-4 Remote Maintenance	No remote maintenance and diagnostics are allowed on an ongoing basis.
MA-5 Maintenance Personnel	Only authorized personnel are allowed to perform maintenance on customer environments
MA-6 Timely Maintenance	<p>Project Hosts has a trouble ticketing system in place that allows efficient management of any escalations that may be required to resolve an issue as quickly as possible. In the ticketing system, issues are categorized as follows:</p> <ul style="list-style-type: none"> a. Emergency. This is for site down or pending site down situations. It applies to situations that will affect all users in the deployment. b. Change. This is to change some configuration of the environment. For example to request a restore of the previous days database backup. c. Upgrade. This is to install some new software or integrate with another location. <p>The time required to resolve an issue varies depending upon the nature and severity of the issue. Standard resolution times are:</p> <ul style="list-style-type: none"> a. Emergency: 0 – 2 hours b. Change: 2 – 4 hours, or possibly more depending on the nature of the change. c. Upgrade: Project Hosts typically requires 5 business days to implement an upgrade, but more time could be required, depending on the nature of the upgrade.
Media Protection	
MP-1 Media Protection Policy	The CTO's office maintains standard policies and procedures for media protection.
MP-2 Media Access	Only authorized company personnel are allowed media access.
MP-3 Media Labeling	Does not apply

MP-4 Media Storage	Information system media is maintained in a secure data center with 24/7 onsite security under physical lockdown. On the standard offering data is not encrypted on a backup tape. If customer requests this option, Project Hosts can accommodate accordingly.
MP-5 Media Transport	Only authorized company personnel may transport media outside of controlled areas.
MP-6 Media Sanitization and Disposal	All media are erased and recycled as needed.
Physical and Environmental Protection	
PE-1 Physical and Environmental Policy	Physical and environmental policies and procedures are in place and maintained by our hosting service provider, Qwest.
PE-2 Physical Access Authorizations	A list of authorized personnel is maintained and transmitted to our data hosting centers to limit access to authorized personnel only
PE-3 Physical Access Control	Qwest maintains physical site security. Qwest CyberCenters are outfitted with biometric palm scanners and secure card-key access to the collocation areas of the data center. Additionally, all customer equipment is kept in secure locations. On-site security personnel monitor hosting facilities 24/7 via indoor and outdoor video surveillance. CyberCenter access requires security desk check-in and is managed 24/7.
PE-5 Access Control for Display Medium	All servers are stored in locked cabinets that can only be accessed when unlocked by authorized Qwest personnel
PE-6 Monitoring Physical Access	Qwest maintains physical site security. Qwest CyberCenters are outfitted with biometric palm scanners and secure card-key access to the collocation areas of the data center. Additionally, all customer equipment is kept in secure locations. On-site security personnel monitor hosting facilities 24/7 via indoor and outdoor video surveillance. CyberCenter access requires security desk check-in and is managed 24/7.
PE-7 Visitor Control	Qwest maintains physical site security. Qwest CyberCenters are outfitted with biometric palm scanners and secure card-key access to the collocation areas of the data center. Additionally, all customer equipment is kept in secure locations. On-site security personnel monitor hosting facilities 24/7 via indoor and outdoor video surveillance. CyberCenter access requires security desk check-in and is managed 24/7.
PE-8 Access Records	Qwest maintains a full physical log of visitors
PE-9 Power Equipment and Power Cabling	Power is available as needed. It is designed with battery backup for uninterrupted power supply (UPS). Diesel generators (N+1) ensure uninterruptible power.
PE-10 Emergency Shutoff	Does not apply
PE-11 Emergency Power	Power is available as needed. It is designed with battery backup for uninterrupted power supply (UPS). Diesel generators (N+1) ensure uninterruptible power.
PE-12 Emergency Lighting	Does not apply
Pe-13 Fire Protection	All CyberCenters are designed with N+1 redundant chilling/heating systems and redundant, multi-zoned, fire suppression systems. Very Early Smoke Detection Apparatus (VESDA®) systems are located throughout the raised floor area in all CyberCenters.
Pe-14 Temperature and Humidity Controls	All CyberCenters are designed with N+1 redundant chilling/heating systems
PE-15 Water Damage Protection	Qwest maintains data center control of water damage protection.
Pe-16 Delivery and Removal	Does not apply
PE-17 Alternate Work Site	Does not apply
PE-18 Location of Information System Components	Does not apply
PE-19 Information Leakage	Does not apply

Security Planning Policy	The CTO's office maintains standard policies and procedures covering system security.
System Security Plan	A security plan for the information system provides an overview of the security requirements and is maintained and enforced by the CTO.
System Security Plan Update	The CTO reviews and updates the security plan periodically.
Rules of Behavior	Rules of behavior would normally be implemented by the client CRM system administrator, not by Project Hosts.
Privacy Impact Assessment	A privacy impact assessment of the information system would normally be completed by the client CRM system administrator or other designated client representatives.
Security related Activity Planning	
Personnel Security	
PS-1 Personnel Security Policy	Standard procedures and policies are in place to guide personnel security.
PS-2 Position Categorization	Risk designations are applied to all relevant positions and screening criteria are applied for new hires to each position.
PS-3 Personnel Screening	All Project Hosts employees have an initial background check prior to employment and are periodically screened thereafter. All background checks are completed by a third-party (Execustaff Inc.).
PS-4 Personnel Termination	Upon termination, employee system access is revoked and all related property is returned.
PS-5 Personnel Transfer	Upon transfer, the access authorization of an employee would be reevaluated and changed accordingly.
PS-6 Access Agreements	All employees have to sign confidentiality agreements protecting client information.
PS-7 Third Party Personnel Security	Does not apply
PS-8 Personnel Sanctions	Does not apply
Risk Assessment	
RA-1 Risk Assessment Policy	The CTO's office maintains risk assessment policies and procedures and assures they are applied as needed.
RA-2 Security Categorization	Security Categorization is Moderate
RA-3 Risk Assessment	The client organization would typically conduct a risk assessment of the magnitude of harm that could result from unauthorized system access.
RA-4 Risk Assessment Update	An update of the risk assessment would be completed upon significant change to the environment.
RA-5 Vulnerability Scanning	
System and Services Acquisition	
SA-1 System and Services Acquisition Policy	The CTO's office maintains system and service acquisition policies and procedures that control new acquisitions.
SA-2 Allocation of Resources	Does not apply
SA-3 Life Cycle Support	Does not apply
SA-4 Acquisitions	Does not apply
SA-5 Information System Documentation	System manuals and/or instructions are provided upon delivery of deployments
SA-6 Software Usage Restrictions	Project Hosts complies with all applicable software usage restrictions
SA-7 User Installed Software	Does not apply
SA-8 Security Engineering Principles	Does not apply
SA-9 External Information System Services	Qwest is our External Information System services provider for data backup and Internet access. Agreements are in place with Qwest regarding network access, services, and physical and network security policies.
SA-10 Developer Configuration Management	

SA-11 Developer Security Testing	Project Hosts does not do any development. We only install Microsoft CRM. Therefore, the Developer Security Testing does not apply to Project Hosts.
System and Communications Protection	
SC-1 System and Communication Protection Policy	The CTO's office maintains and enforces system and communication protection policies and procedures.
SC-2 Application Partitioning	Application administration access is separated from server administration access to partition access between those needing access to the application and those needing admin access to the IT system
SC-3 Security Function Isolation	
SC-4 Information Remnants	The server is dedicated specifically to customer. Therefore, the ISS and CRM prevents information remnants reuse.
SC-5 Denial of Service Protection	Provided via the system's Cisco PIX firewall
SC-6 Resource Priority	
SC-7 Boundary Protection	Boundary protection is provided via the system's Cisco PIX firewall. Firewall configuration settings are normally not released to protect the overall security of the network. We will explore limiting access to the server from a fixed range of IP addresses with our CTO to determine the feasibility. IIS server can be configured to only accept requests from a designated IP address range. There is no additional charge for this modification.
SC-8 Transmission Integrity	Transport security: All communication between your PC and your hosted CRM environment is made through SSL. This protocol employs 128-bit encryption to protect your data in transport.
SC-9 Transmission Confidentiality	Transport security: All communication between your PC and your hosted CRM environment is made through SSL. This protocol employs 128-bit encryption to protect your data in transport.
SC-10 Network Disconnect	No network disconnect is normally available. A network disconnect could be implemented for non-administrator web browser users, if required, for an additional charge . However, if non-administrator users are only allowed to access the system through their Outlook client, then our understanding is that this requirement will be met by the existing customer client PC security measures.
SC-11 Trusted Path	
SC-12 Crypto Key Establishment and Mgmt	Transport security: All communication between your PC and your hosted CRM environment is made through SSL. This protocol employs 128-bit encryption to protect your data in transport.
SC-13 Use of Validated Crypto	Transport security: All communication between your PC and your hosted CRM environment is made through SSL. This protocol employs 128-bit encryption to protect your data in transport.
SC-14 Public Access Protections	Does not apply
SC-15 Collaborative Computing	Does not apply
SC-16 Transmission of Security Parameters	
SC-17 Public Key Infrastructure Parameters	All communication between your PC and your hosted CRM environment is made through SSL. This protocol employs 128-bit encryption to protect your data in transport.
SC-18 Mobile Code	Does not apply
SC-19 Voice over Internet Protocol	Does not apply
SC-20 Secure Name/Address Resolution (Authoritative)	Does not apply
SC-21 Secure Name/Address Resolution (Recursive or Caching Resolver)	

SC-22 Arch and Provisioning for Name Address Resolution Service	Does not apply
SC-23 Session Authenticity	Transport security: All communication between your PC and your hosted CRM environment is made through SSL. This protocol employs 128-bit encryption to protect your data in transport.
System and Information Integrity	
SI-1 System and Information Integrity Policy	The CTO's office maintains system and information integrity policies and procedures.
SI-2 Flaw Remediation	Procedures are in place when installing newly released security relevant patches, service packs, hot fixes and test patches. Furthermore, before making changes an administrative access user ("admin") will assess the impact to hardware, networking, operating system, database, application, and client access layers. If changes carry risk of downtime, the admin will do the following: obtain approval from the Customer rep, schedule the change to be made during a maintenance window, and have a backup of the system made before making the change.
SI-3 Malicious Code Protection	McAfee security software is employed and kept continually up to date to ensure a clean, safe environment.
SI-4 Intrusion System Monitoring Tools and Techniques	We currently have Snort Intrusion System Monitoring software in place at this time. We use a Lock Out process that will lock out a particular account that unauthorized external port scans are being used against after 5 attempts. This technique is used in conjunction with other monitoring tools that are in place. See SI-5 We are willing to look into this type of monitoring software if requested by the customer.
SI-5 Security Alerts and Advisories	Project Hosts monitors' application integrity and availability using Site/Scope monitoring system with deep URL content verification and MRTG software for traffic monitoring.
SI-6 Security Functionality Verification	The McAfee security software is monitored for performance on an ongoing basis.
SI-7 Software and Information Integrity	McAfee security software is employed and kept continually up to date to ensure a clean, safe environment and to prevent against unauthorized system access. The Cisco PIX firewall monitors network traffic and creates a traffic log. There is nothing in place that automatically shows whether or not data files or operating system files were tampered with, replaced or created. This process has to be completed, manually.
SI-8 Spam and Spyware Protection	Virus security: McAfee Virus software is employed and kept continually up to date to ensure a clean, safe environment.
SI-9 Information Input Restrictions	Windows security: Project Hosts employs the strictest possible Windows lock-down techniques. Users only have access to the functions required for the functioning of their CRM solution, and they are securely separated from all other users in the data center. All servers run Windows 2003 and any applicable security patches are applied shortly after they become available. Input restrictions from the CRM application is controlled by role based security within the application.
SI-10 Information Input Accuracy and Validity	Does not apply
SI-11 Error Handling	Error logs are only viewable by a Project Hosts system administrator and do not contain sensitive information. The error logs are monitored on specific events as needed.