ARCHIBUS Hosting Services – Technical and Security Information

THE WORLD'S #1 HOSTED SOLUTION FOR TOTAL INFRASTRUCTURE AND FACILITIES MANAGEMENT

TECHNICAL INFORMATION

Version Control

Version	Issue by	Date	Comments / Changes
0.1	Ana Maria Fernandez	DIC 20 2011	Initial Draft
1	Miguel Sánchez Miguel	AUG 10 2011	Approved. Second version. Authorized Hosting Partner Program
2	Miguel Sánchez Miguel	FEB 1 2012	Approved. Separated versions for AoD & AHtd

For any question related to document, please contact:

Ana María Fernández de Simón
CIO and Innovation Manager
Phone : (+34) 926 920 150
Mobile : (+34) 671 660 742
e-mail : ana.fernandez@asc-hs.com

CONFIDENTIALITY

Scope

This document describes the technical aspects and gives information about security procedures and details of the infrastructure to provide the ARCHIBUS Hosting Services.

Table of Contents

Definitions

AHS: *ARCHIBUS Hosting Services / ARCHIBUS Hosting Solutions*, includes: ARCHIBUS On Demand (SaaS model), and ARCHIBUS Hosted (PaaS or condo method).

AHS-AHP: *ARCHIBUS Hosting Services – Authorized Hosting Partner*.

AI: *ARCHIBUS, Inc.* – Proprietary of ARCHIBUS Hosting Services, and the AHS-AHP Program.

ASC-HS: *ARCHIBUS Solution Center – Hosting Services*, is in charge of global management of ARCHIBUS Hosting Solutions and the AHS-Authorized Hosting Partner Program.

AHtd: *ARCHIBUS Hosted*.

AoD: *ARCHIBUS On Demand*.

ARCHIBUS Cloud Computing global framework: The collection of all the ARCHIBUS Hosting Services - Authorized Hosting Partners, working connected, creating a global network all together.

1 ASC-HS Infrastructure

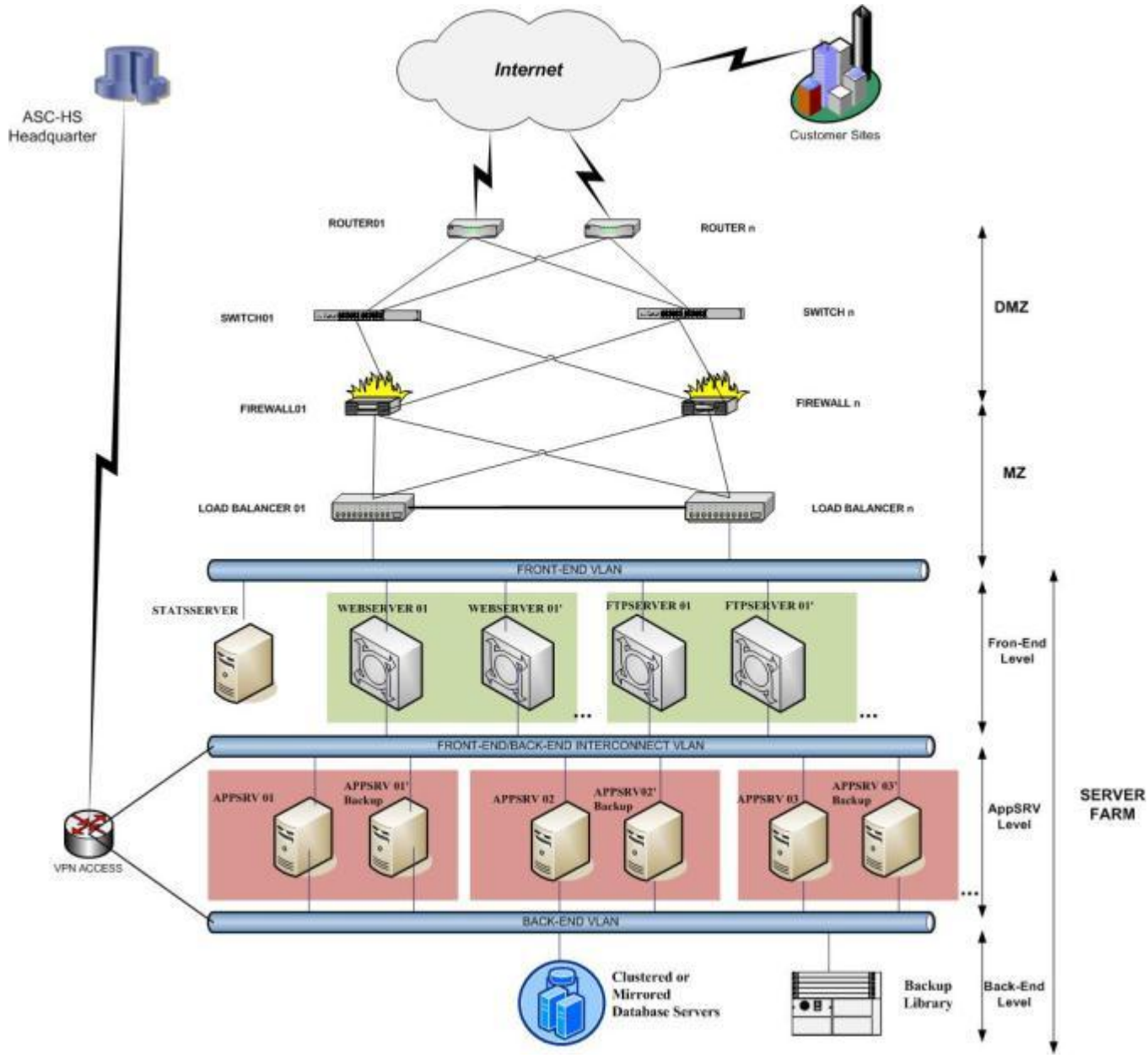
ARCHIBUS Hosting Services is hosted in "ARCHIBUS Authorized Hosting Partners" secure, top-tier data centers. ASC-HS offers a highly secure and reliable carrier-neutral environment to deploy computing, network, storage and IT infrastructure. The world-class NAP data centers help reduce the capital and operational expense required to house and protect applications and systems.

The "ARCHIBUS Authorized Hosting Partners" provide Service Level Agreements (SLAs) for power and environmental systems through a number of redundant subsystems, including power and fiber trunks from distinct sources.

Managed Network and Connectivity services include the most basic layer one services such as physical interconnection all the way through more complex layer three monitoring of networks and alerts. Carrier-neutral design provides zero mile access to robust connectivity and at the same time delivers cost savings, flexibility, and can scale to match customer growth while still delivering the performance customers demand.

Our data centers offers a full line of managed and professional network security solutions, including vulnerability assessments, penetration testing, incident response and customized services to help clients identify, understand, and effectively deal with security issues before and after they occur.

This is the required diagram to provide and support the "ARCHIBUS Hosting Services":


Internet
ASC-HS Headquarter
Customer Sites
ROUTER01
ROUTER n
SWITCH01
SWITCH n
FIREWALL01
FIREWALL n
LOAD BALANCER 01
LOAD BALANCER n
DMZ
MZ
FRONT-END VLAN
STATSSERVER
WEBSERVER 01
WEBSERVER 01'
FTPSERVER 01
FTPSERVER 01'
Fron-End Level
FRONT-END/BACK-END INTERCONNECT VLAN
APPSRV 01
APPSRV 01' Backup
APPSRV 02
APPSRV 02' Backup
APPSRV 03
APPSRV 03' Backup
AppSRV Level
SERVER FARM
VPN ACCESS
BACK-END VLAN
Clustered or Mirrored Database Servers
Backup Library
Back-End Level

1.1 Security Data and Certifications

Our hosting providers (i.e. Terremark in the USA) are certified according to ISO27001 or SAS70 standards. They accomplish with the security rules and follow the rules data protection policies according to EU Directive 95/46/EC.

ARCHIBUS Hosting Services are based on ARCHIBUS, a TIFM (Total Infrastructure and Facilities Management) solution. Depending on the contracted applications or modules, all the loaded data in ARCHIBUS Hosting Services system is related with customer's infrastructure and general customer's data which identifies companies. Some examples are: Company name, contact customer name, contact customer last name, address, telephone, mail, etc. ARCHIBUS Hosting Services also can load general employee information.

1.1.1 Privacy Policy

"Data Protection Directives" means the European Union Directive entitled "Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" and the European Union Directive entitled "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector"; For the purposes of this section, "personal data", "special categories of data", "process/processing", "controller", "processor", "data subject" and "supervisory authority" shall have the same meaning as in the Data Protection Directives. "Data Protection Legislation" means any legislation in force from time to time which implements the Data Protection Directives and is applicable to the provision of the ARCHIBUS Hosting Services.

ARCHIBUS Solution Center Hosting Services doesn't collect any personal information. We just collect the contact information for administrative and support purpose. You can contact or send an email to privacy@asc-hs.com to resolve any concern or question about privacy policies.

The complete privacy policy is published in the following link: http://www.asc-hs.com/online-privacy-policy

1.2 Information Security

ASC-HS datacenter has implemented controls to provide network based security measures to protect its enterprise network. A security policy is in place and a security awareness program is designed to educate employees to protect ASC-HS's network and systems. A variety of hardware and software based tools have been deployed, which include firewalls, intrusion detection systems, routers, switches, real-time monitoring, and audit logging.

Redundant and clustered industry standard firewalls, switches and routers are implemented to provide a high level of availability and security of network, applications and data. In clustered firewall/router implementations, if one system fails, data traffic is automatically routed to the other standby firewall/router. Configuration standards of firewalls and routers are documented. The configuration of the firewall systems follow vendor recommendations and are based on the principle of least privilege, which allows only necessary and authorized access and denies other services and protocols. The firewalls are strategically placed on the network to filter data packets according to predefined access rules. Administrative access to networking devices is limited to authorized IT personnel only.

The enterprise network is segmented and grouped into different virtual local area networks (VLAN) based on business functions and responsibilities. The VLANs are built by deploying industry standard switches and the proper configuration and administration. Network segmentation serves as an additional security measure to minimize risks resulting from unauthorized network access.

A third party company is engaged to perform quarterly vulnerability assessments for a portion of its publicly accessible IP addresses. The IT personnel review the scanning reports to assess and remediate potential network and system vulnerabilities.

The ASC-HS's team performs annual penetration tests scan against the management environment and reviews the results and remedies potential network and system vulnerabilities.

1.3 Security Incident response

ASC-HS maintains a security incident response plan in order to organize resources to respond in an effective and efficient manner to an adverse event related to the safety and security of a computer resource under ASC-HS's management. An adverse event may be malicious code attack, unauthorized access to managed networks or systems, unauthorized utilization of ASC-HS services, denial of service attack, or general misuse of systems.

An incident response team is in place with defined roles and responsibilities. The purpose of this team is to protect ASC-HS and its customers' information assets, provide a central organization to handle Incidents, comply with government or other regulations, prevent use of ASC-HS managed systems in attacks against other systems, and minimize the potential for negative exposure. Major responsibilities of this team include:

- Limiting immediate incident impact to customers and business partners
- Recovering from the incident
- Determining how the incident occurred

• Determining how to avoid further exploitation of the same vulnerability

• Avoiding escalation and further incidents

• Assessing the impact and damage

• Determining the cause of the incident

• Compiling and organizing incident documentation

• Reviewing response to incidents

• Updating policies and the Security Incident Response Plan

Security incident occurrences are tracked and documentation is maintained. Actions and procedures are documented to guide the incident response team to respond in the event of a security incident and include:

• Taking control of the incident and invoking the security incident response plan

• Assigning an incident response coordinator, communication manager, and technical account manager and starting documentation of the incident report including personnel assignments

• Notifying the security manager on duty at the time of the incident

• Assessing the incident

• Reporting findings to the communications manager

• Communicating the incident to the incident response team, customer, and identified additional personnel including external agencies as appropriate, and maintaining communications throughout the life of the incident

• Containing the damage and minimizing immediate exposure

• Identifying the impact of the incident

• Remediation of the vulnerabilities

• Collecting and protecting evidence

• Recovering the systems

• Preparing the incident analysis report for trending and analysis

• Preparing and presenting the incident summary as necessary to the customer

Once the documentation and recovery phases of the incident are complete, the team thoroughly reviews the process that was followed during the incident to determine what was successful and where mistakes were made. Based on findings, policies and the plan are updated as appropriate.

1.4 Infrastructure system monitoring and support

Our hosting providers (i.e: Terremark in the USA) provides monitoring 24/7/365 of ASC-HS and clients' networks and system infrastructure for continuous system performance and signals of system failure.

The ASC-HS providers tests monitoring redundancy several times each day. Another method of monitoring notification specifically for network engineers includes alerts firing through the network monitoring information system (NMIS). When an alert fires in NMIS, an e-mail is sent to the network operations engineer team.

A shift manager is on duty to provide proper supervision on each shift during the week and is on call on weekends if issues arise. A monitoring engineer cannot leave his/her monitoring station until being replaced with another monitoring engineer.

The system performance items monitored by the ASC-HS include:

• Disk space usage, CPU, memory, NIC utilization, back up successes and failures

• Thresholds for CPU utilization, networking device interface utilization, and interface up/down status

• Keyword monitoring (URL and IP), ping-based connectivity monitoring for all devices

• Server hardware monitoring, predictive fault detection

When an alert is triggered, a monitoring engineer creates and assigns a service call to the team responsible for responding to the incident. All engineers take actions following alert handling procedures and incident resolution procedures. The incidents are tracked to resolution using service calls within the support console.

1.4.1 System Data Backup Procedures

ASC-HS backs up the files and data on all servers in order to ensure a fast recovery of services in the event of a hardware/software failure or physical disaster. To make these services available, the files on each system are regularly copied to a recovery storage medium and retained for various periods of time. ASC-HS has established formal procedures to manage data backup and backup media operations.

ASC-HS uses the following backup schedules:

• Weekly full backups are run according to the server backup schedules. The weekly full backup tapes are clearly labeled and kept onsite in fireproof containers for two weeks.

• Daily incremental backups are run each day between the regularly scheduled full backups. The daily incremental backup tapes are clearly labeled and stored onsite for easy and fast recovery.

The backup is automated using third party backup software utilities, which provide reports on successful and failed jobs, status and run times. A backup verification process is run on each file after the backup occurs to ensure the data integrity of the tape. The daily backup job status for each system is monitored and service calls are created in service desk for every failure or exception reported by the backup process.

The customer support incident management team provides Level 1 support for standard backup failures and escalates to Level 2 if they are unable to resolve the problem. Exceptions to this standard backup process are documented in the return to service documentation specific to customer systems as applicable. This procedure allows systems to be restored in the event of a disaster. Individual files can be restored if they were present on the system during a backup operation.

Backup tapes are replaced when an error due to bad media is detected during the backup process. Any defective media, including defective tapes, are logged into the Tape Disposal Log and dispatched for physical destruction. RAID technologies are implemented according to customer's requirements to reduce the risk that a disk problem could bring down the entire system. RAID (Redundant Array of Independent Disks).

ASC-HS made a backup of the following files to provide ARCHIBUS Hosting Services:

1. **ARCHIBUS Application Files**: Files included into the ARCHIBUS default directory
2. **Client/s Project/s**: Files included into
3. **Web Central Files:** Files included into

Databases. Weekly full backups and daily incremental backup

- Backups are done when servers are at their minimum activity period in order not to interfere with their current performance.
- One daily completed backup should be done.
- Fortnightly copies are stored; therefore data can be restored as it was any previous day before backup was done.

ASC-HS allows customers to request a backup restore of ARCHIBUS Hosting Services solutions. ASC-HS requires a request from customer with a minimal of 2 hour since the request is done.

This task will be done in the following cases:

- Copy or restore when customers request it.
- Restore for critical incident.

The restore should be done taking into account this condition:

- ASC-HS will restore the backup in working days and if this action not affects the customer. In other case, it is needed to do it at non-working hours.
- The executed backup restore has the same format, recovered files & directory structure as it appears in the backup procedure.

1.5 System Software Maintenance

ASC-HS utilizes many information system software products from a variety of vendors. These software products include operating system software, database system software, networking system software and other middleware applications. Software product vendors produce new releases, service packs, and hot-fixes to enhance the software's functionality and security. It is important for ASC-HS to be notified of, evaluate, package, test, and implement vendor patches and updates to maintain a high level of functionality and security of its network and hosted systems for clients. ASC-HS has established a patch management process to guide evaluation, testing, and implementation of vendor system software patches.

ASC-HS's Team is notified of software updates in several ways including vendor provided automatic system update services, vendor notification mailing lists, and industry-specific mailing lists. For example, new security patches for the Microsoft platform are released the second Tuesday of each month. Once these patches are released, ASC-HS receives an e-mail notification from Microsoft. Microsoft also sends ASC-HS an e-mail notification of any emergency patches released prior to the second Tuesday of each month. Another example, ARCHIBUS send an e-email with notification of the software updates.

ASC-HS's evaluates the criticality and applicability of the updates. Based on the rating of the patch by the vendors and how it affects the hosted server-based solutions, ASC-HS determines whether the patch is required or not.

Each patch is tested in a non-production environment to ensure the patch's functionality and operability with the standard system settings. The technical people group then creates a report detailing an advisory of possible effects, installation procedures, and back-out procedures to guide patch implementation on production systems. Once testing is complete, the patches are released to Change Management for scheduling and deployment to production. The actual patch installation follows ASC-HS's change management procedures.

1.6 Business continuity planning and recovery

Planning for business continuity in the event of a disaster is a regular part of ASC-HS's operations. ASC-HS ensures regular backups, secure onsite and offsite storage of data, and the ability to recover data quickly. All customer stored data backup are separately stored in our systems.

In the event of a disaster, ASC-HS's business continuity plan details how operations will be re-established. The plan takes into account multiple disaster scenarios that could happen such as loss of power, loss of facility, and pandemic flu, to name just a few. The plan then details the steps that would occur to ensure business continuity in each of those various scenarios. Essential personnel, tools, technologies, facilities, and processes are considered and contingency plans are discussed, documented, tested, and implemented. The plan is updated at least once annually, and often more frequently as new technologies warrant business continuity planning or the environment changes.

1.6.1 Business Continuity Activities

ASC-HS tests different scenarios of its Disaster Recovery/Business Continuity plan at least annually.

Other areas of the business continuity plan are enacted during the year through interrupted business operations. Business continuity activity includes the following:

Backup and Restore of Data Files and Libraries: ASC-HS backs up files and data on specified servers, to ensure a fast recovery in the event of a hardware/software failure or a physical disaster. This also provides a measure of protection against human error or inadvertent deletion of files. There are weekly full backups, daily incremental backups, and a backup verification process to ensure data integrity to tape. The backup process ensures that the most current backup and a previous week's backup are available within the data center, and ensures the previous two weeks of backups are in offsite storage. ASC-HS regularly restores data for its clients from backups.

Plan Activities

The following updates are made as part of the Disaster Recovery / Business Continuity Plan:

- Business Continuity Team Leaders are reviewed and updated
- Vendor and employee list are made current

1.7 Control Environment

1.7.1 Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of ASC-HS's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of ASC-HS's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well by example. Specific control activities that the service organization has implemented in this area are described below.

- Documented organizational policy statements and codes of conduct are in place to guide personnel in integrity and ethical practices that include, but are not limited to, the following:
    - Employment, pay and benefits
    - Work policies and regulations
    - Conflicts of interest
- Employees and third party contractors are required to sign an acknowledgment form indicating that they have been given access to the security manual and understand their responsibility for adhering to the policies and procedures contained within the security manual.
- Employees and third party contractors are required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
    - Employees/third party contractors are required to sign an acknowledgment form indicating that they have been given access to the computer, e-mail, and Internet usage policy.
    - Background checks are performed for employees as a component of the hiring process.

1.7.2 Authentication, Authorization, Accounting

ARCHIBUS uses the Spring Security Framework for authorization management. This framework supports many authentication models, and has been used in live deployments with Site minder. The framework is also extensible to meet requirements that may not be available out of the box and it can be integrated with SAML 2.0 software for authorization. **(**e.g. Integrity Site minder)

The ARCHIBUS password policies includes at a minimum policies related to administrative passwords, time for required changes, length and complexity, first time usage, lockouts, communication of passwords to employees, how to reset passwords.

In order to enforce consistent password policies, ARCHIBUS requires you to have one consistent encoding for all passwords. You establish this encoding before you start Web Central, and at that point, all legal passwords must be in that current encoding.

In order to achieve the desired level of security on passwords, ARCHIBUS supports encodings that cannot be reversed, meaning that once a password is encrypted, you cannot retrieve the original password. As such, in order to change encodings, you must issue a new password to all users. For this reason, ARCHIBUS has features to:

- Bulk-generate unique plaintext password for each user
- Email plaintext passwords that must be changed on first login
- Bulk-encrypt plaintext passwords

In particular, the following are typical transitions and the method you would use:

- Plaintext to ARCHIBUS-encoding. Since your current passwords are not encrypted, you can simply encrypt them. End users can log in with the same passwords (as the storage format of the password has changed, but not the original password itself).
- Plaintext to SHA. Since your current passwords are not encrypted, you can simply encrypt them. End users can log in with the same passwords.
- ARCHIBUS-encoding to SHA. Since your passwords are encrypted, you must generate new passwords for your users, email them to your users, then encrypt the new passwords.
- SHA to ARCHIBUS-encoding. Since your passwords are encrypted, you must generate new passwords for your users, email them to your users, then encrypt the new passwords.

1.8 ASC-HS Server Farm

The ASC-HS is a distributed computing platform, so it's structured as in three different levels: front-end, application and back-end:

- In the front-end, there is the farm of "web" and "ftp servers". Both are redundant and load balanced. In the same level, there also is the "stats server" where the partner can provide information about the ARCHIBUS Hosting Services use.
- Below is the ASC-HS **application** server farm level. Application servers type offered are: PRODUCTION Server, TEST-DRIVE Server, QA Server (Quality Assurance), DEMO Server, and TRAINING Server. The access to these servers is only through the Front-end level. PRODUCTION Servers (only) must have active / passive clone back-up server.
- The backend level ASC-HS must include:
    - The Database cluster, which doesn't have access from Internet and it will be only access through application level.
    - The back-up infrastructure.

For the web and ftp farms, ASC-HS allow the use of different technologies, but all the serves must be implemented with load balancing and fault tolerance. The Web servers must be able to filter all the malformed requests to the system.

The "application infrastructure level" is based on virtual servers, that mean the ARCHIBUS application servers so implemented, allows to move and migrate those virtual machines between different physical servers without outage. Virtualization facilitates the growth and updates of the servers in the case of project and system requirements changes over time.

To implement the entire infrastructure, a secured back-end infrastructure is necessary, which provides a database cluster and a back-up system.

Data Base Management servers are "physical servers" connected to the SAN (Storage Area Network) in order to offer high levels of performance and fault tolerance. It is mandatory not to use virtual server for the Data Base cluster.

In the back-end layer, a backup infrastructure must be included where the ARCHIBUS Authorized Hosting Partner provides the customer backup required as according to the ASC-HS procedures.

1.9 ARCHIBUS Hosting Services Deployment

All applications are installed on an additional partition which is independent of the operating system default C:\)

The deployment workflow is:

1. (optional) **DEVELOPMENT Server** – Remotely accessible with all the control (Web + Terminal Server Admin) by ARCHIBUS Business Partner (Implementer)
2. (optional) **QUALITY ASSURANCE Server** – To test all changes in the projects before PRODUCTION – Remotely accessible by End Customer (Web) and ARCHIBUS Business Partner (Web + Terminal Server Admin)
3. **PRODUCTION Server** – Only accessible through Web, directly to ARCHIBUS Web Central Project. There are two types:
    a. **PRODUCTION SHARED Server –** Project is isolated in its own Application Server but sharing Server with other Projects (App Servers instances) in the same machine. In this scenario **Database** must be allocated in external cluster.
    b. **PRODUCTION DEDICATED Server –** Project is installed and hosted in a proper and isolated virtual Server. **Database** engine for small projects can be hosted in the same machine.
4. (optional) **DATABASE Cluster –** This infrastructure, is an external cluster (MS SQL Server or Oracle) to host Project Databases.

2 Reponses to fill up Third Party formularies

Number	Name	Answer
11.1	**Overall**	
11.1.1	Does your company provide your solution in a SaaS model?	Yes
11.1.2	Do you have partners who offer your solution in a Saas model? If so please list the partners.	ARCHIBUS On Demand (SaaS) is offered exclusively through the ARCHIBUS Solution Center- Authorized Hosting Services Partners ecosystem.
11.2	**General security**	
11.2.1	Do you regularly perform vulnerability assessment on your production environment? (Pl. provide details - like frequency, who performas assessment etc.)	To be in compliance with the security certification (ISO 27001, SAS70). Our ARCHIBUS Hosting Partners run quarterly internal and twice-a-year external intrusion vulnerability tests.
11.2.2	Do you allow customer initiated audits of the Application Infrastructure? (Pl. provide details)	Yes. Physical visit to the hosting premises can be arranged. A 30-day notice is required.
11.2.3	Is it possible to immediately disable all or part of the functionality of the application should a security issue be identified?	Yes
11.2.4	How long after termination of business agreement would you keep copies?	30 days
11.2.5	Please describe how Information Security is handled in your organization.	Information security is handled according to our Authorized Hosting Partners' certified/accredited with an Information Security Management System (ISO 27001 or SAS70).
11.2.6	Please show how security fits within your company's organizational structure?	As an ISO 27001 certified organization our ARCHIBUS Solution Centers - Hosting Services require from its partners and providers to comply with security at all levels in production and delivery
11.3	**Physical Security**	
11.3.1	List the physical security controls managing access to systems and networks housing or processing data.	All our hosting facilities are Level 2 or 3.
11.3.2	Some customer policy requires that every person who has access to customer data must have a background check performed. Does your company do background checks of all employees that would have access to customer's data?	Yes, all employees do background checks and they also have signed the confidential and security agreements.

11.4	**Authentication, Authorization, Accounting**	
11.4.1	Is your software able to integrate with external Ping Federated or other SAML 2.0 software for authorization (e.g. Netegrity Siteminder)?	Yes, refers to the Authentication, Authorization and Accounting section of this document.
11.4.2	Please describe your password policies. Include at a minimum policies related to administrative passwords, time for required changes, length and complexity, first time usage, lockouts, communication of passwords to employees, how to reset passwords.	Go to the "Authentication, Authorization and Accounting" section of this document.
11.4.3	Are passwords on network devices and systems encrypted?	Yes
11.4.4	What is the termination procedure for user credentials?	1 Request from the client to terminate user account 2 Transfer data to another user account if proceeds 3 Delete terminated user from ARCHIBUS application 4 Delete user from LDAP (hosting only)
11.4.5	How is data protected from access by your employees?	All customer data is accessed only through the ARCHIBUS application. Our employees have no user accounts in the ARCHIBUS application. The client has the user account control.
11.4.6	List all groups that have access to data and their respective roles.	Only the ARCHIBUS.system admin group
11.4.7	How do you maintain and process your logs?	All ARCHIBUS logs can be accessed from inside the application by users with the right credentials. All login attempts are logged by the server according to the application and Log4J configuration settings.

11.5	**Network Security**	
11.5.1	Is it possible to provide an infrastructure that is isolated from other customer's infrastructure as well as the vendor's corporate environment?	On the SaaS model we offer shared and dedicated (private cloud) environments. The dedicated model isolates the customer infrastructure.
11.5.2	Please indicate all network security controls protecting infrastructure related to the customer environment	See the ASC-HS Infrastructure section of this document.
11.5.3	Does the proposed solution use the internet, a private link, or a combination of the two for transmission of data? This should be reflected in the data flow diagram.	Mainly Internet. But in some cases where the customer requires a special configuration or access, a private link or VPN can be set up for data loading and/or administration purposes
11.6	Host Security	
11.6.1	Do you have hardening guidelines for servers? None Internally Developed Guidelines Public Standard Guidelines:	We have hardening policies: Periodic Intrusion tests and check the user directory and logins.
11.6.2	How do you keep up on security vulnerabilities?	With a three tier DISA structure deployment
11.6.3	What is the policy and procedures (including QA) for installing security patches?	**Refers to the "System Software Maintenance" of this document.**
11.6.4	Would you be willing to supply documentation of your current patches on customer related equipment with security personnel?	Yes
11.6.5	How is the integrity and availability of the hosts and applications monitored?	Monitored through control systems deployed by our hosting providers (i.e. Terremark in the USA).
11.7	**Backups and Disaster Recovery**	
11.7.1	Describe your backup procedure including: frequency, encrypted?, frequency of verification, disposal of backup media.	Refers to "System Data Backup procedures" section in this document.
11.7.2	Do you have a disaster recovery plan?	Yes
11.7.3	What is your disaster recovery model? Hot Warm Cold	Refers to "Business continuity planning and recovery" section in this document.
11.7.4	Does your disaster recovery plan include provision for the customer related operations and data?	Yes
11.7.5	For backups of systems dealing with Customer data, is the data stored separately from other customer data?	Yes

11.7.6	Can customer data be recovered separately from other customer data?	Yes
11.8	**Application**	
11.8.1	Describe your application account creation process? Who creates the accounts? How is the need for an account validated?	Once the service is activated, the client's system admin personnel can create user accounts and assign business roles to them within ARCHIBUS.
11.8.2	Do you have procedures on identifying and mitigating social engineering attacks?	The security framework, including intrusion and deterrence systems, identify and address any thread coming from the outside.
11.8.3	How do you audit and verify active accounts?	Creating, editing and terminating accounts in ARCHIBUS is an end-user's responsibility.
11.8.4	How are application user passwords stored? What type of encryption, if any, is used for password storage?	In ARCHIBUS, the end-users' passwords are encrypted at the data level. ARCHIBUS Web Central can use different password encodings: Plaintext. This is the default encoding that ARCHIBUS ships with so that the sample database and new projects load and run. ARCHIBUS-encoding. This is the ARCHIBUS 2.0 encoding that has been in use for all of the Web Central releases. SHA. (Secure Hash Algorithm) A one-way hash devised by the National Security Agency and published by the National Institute of Science and Technology as a Federal Information Processing Standard. The default strength used is SHA-1, although you can change the strength to SHA-256, SHA-384, and SHA-512. Tailored encoding. If you are familiar with Spring Security, you can substitute your own encoding (e.g. MD5).
11.8.5	Can your application use SSL for all application transactions?	Yes
11.8.6	Does the application use Java, JavaScript, ActiveX, PHP, or ASP (active server page) technology?	Java and JavaScript and JSP
11.8.7	What language is the application back-end written in? (C, Perl, Python, VBScript, etc.)	Java
11.8.8	Describe the process for doing security-specific Quality Assurance testing for the application. (For example, testing of authentication, authorization and accounting functions, as well as any other activity designed to validate the security architecture.)	ARCHIBUS Quality Assurance has a series of authentication configurations, test data, user roles, and access rights which they use with a large number of test scripts for testing authentication, SSL, password encryption, UI-process security, field-level and record-level data access security, and defense against illicit SQL access.

11.8.9	Does your ASP solution have all of the following procedures documented: a maintenance patch schedule, a process for applying maintenance patches, and a testing process for testing patches before applying them?	Yes, this is part of the ISO 27001 certification.
11.8.10	Please indicate if your ASP has application code security controls to mitigate these common web attacks: 1. Use of and tampering with hidden fields 2. Cookie or parameter poisoning or hijacking 3. URL parameter tampering 4. Variable checking within application code 5. Buffer overflows within application code 6. Cross site scripting 7. SQL Injection	Yes, the ARCHIBUS code in Web Central controls and mitigates against Web attacks, including each of the attacks mentioned.
11.9	**Privacy**	
11.9.1	Provide your Privacy Policy	http://www.asc-hs.com/online-privacy-policy/
11.9.2	As an international company operating in many different countries. Please detail all privacy laws you are able to comply with. GLBA, EU Privacy, Safe Harbor.	See details in the section “Privacy Policy” of this document.
11.9.3	What Personal information is collected and why? (if any)	Just project's contact information for administrative and support purposes
11.9.4	What is the contact information for users to report privacy concerns/questions? Who responds to this?	privacy@asc-hs.com; support@asc-hs.com
11.9.5	What is your process for notifying customers of any potential breach of security?	When a security breach is discovered, we shut down the service and inform the customer through our Customer Project Manager.