Attachment D. Angel.com’s Information and Site Security Management Policies

Angel.com, a subsidiary of MicroStrategy, is a leading provider of on-demand IVR (interactive voice response) and inquiry response center solutions.

Security Program Management

Information and Site Security Management

An individual should be appointed to coordinate the information security arrangements of the computer installation, to ensure that security activities are carried out in a timely and accurate manner and that security issues are resolved effectively.

Please note that all Angel.com security policies are compliant with the PCI Data Security Standard.

Criteria	Response
Who is responsible for managing the data center physical configuration and security measures?	Director, Facilities, MicroStrategy
Who is responsible for managing physical access (installation owner)?	Director, Facilities, MicroStrategy
How are those activities coordinated (who determines what information is housed where)?	Director, Facilities, MicroStrategy, in conjunction with CIO, MicroStrategy, and CTO, Angel.com
How often do the installation owner and security owners review access procedures?	Once a year
How often does the security manager review information and access privileges with information owners?	Twice a year
Who is responsible for training security personnel on current procedures?	CTO, Angel.com for Angel.com BU employees; CIO, MicroStrategy for all other MicroStrategy employees

Physical Security Controls

Physical Protection

All buildings throughout the enterprise that house critical IT facilities (e.g., data centers, network facilities, and key user areas) should be physically protected against accident or attack, to restrict physical access to authorized individuals and ensure that IT facilities processing critical or sensitive information are available when required.

Criteria	Response
What are the physical access controls?	Badged access to elevators, floor entry, data center entry. Cage with key, racks with keys.
How is information classification reflected in access controls?	The entire Angel.com data center falls under the scope of our PCI compliance.
Who is responsible for training data center personnel on current procedures?	Director, Data Center Operations, Angel.com
How are technological and human controls employed (i.e., where are they located)?	For a person to gain access to the data center, he/she must have a badge with clearance to enter the elevators, open the fourth-floor access doors, open the data center door, and have a key to the Angel.com cage. For a person to gain electronic access to the data center, he/she must connect to the Angel.com network and initiate a VPN session using two authentication factors.
How do access controls respond to emergencies?	Access control to Angel.com facilities during emergencies is coordinated by the SOX Business Continuity Plan of MicroStrategy
How are media secured?	Media are secured within a locked key cabinet at the Angel.com cage.
How are the company resources segregated on a multi-operation site?	Angel.com has a site at its headquarters in McLean and a private cage at an Equinix collocation facility in Ashburn. Physical access to Equinix Ashburn is as per Equinix standard procedure (hand scanner, cage key).
What hardware disposal processes are in place?	Hardware disposal is done through MicroStrategy’s master IT asset management, which falls under its policies. All hardware with media is reimaged before disposal.
Where are the documented procedures maintained?	MicroStrategy Information Services maintains SOPs in its corporate Intranet, and Angel.com augments this set with PCI-specific compliance procedures, which are outlined in an internal collaboration workspace for operations personnel.

Physical Access Controls

Physical access to critical computer installation facilities should be restricted to authorized individuals, to prevent services being disrupted by loss of or damage to equipment or facilities.

Criteria	Response
What levels of access controls are employed?	Data center access is restricted to operations personnel up to VP, Technology and Operations, MicroStrategy Information Services designated security personnel and Director, Facilities, MicroStrategy. All other employees can only gain access to the office floors.
How are data center visitors managed?	Visitors to the data center must at all times be accompanied by a member of the operations staff.
Is outside equipment allowed in the data center?	Generally, no. We maintain a database monitoring appliance from a third-party vendor. This vendor has agreed to all our PCI policies, and we personally vet all its personnel with database access.
How is information confidentiality protected?	Information confidentiality is governed by our PCI compliance requirements and by our privacy policy.
Are additional controls applied to more critical information?	We have special controls regarding “Personal Cardholder Data” as per the PCI Data Security Standard.

Physical Access Privileges

All users of the computer installation should be assigned specific privileges to allow them to access particular information or systems, to provide authorized users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

Criteria	Response
How are access privileges granted, reviewed, and monitored?	Access privileges to the data center can only be granted by the Director, Facilities, upon approval of the Director, Data Center Operations.
How are access privileges requested?	Via an Information Systems Helpdesk request.
How are access requests assessed?	Access requests are assessed based on a merit basis.
How are access privileges approved?	Director, Data Center Operations, and Director, Facilities.
What is the revocation process?	Any authorized facilities personnel may revoke employee credentials.
What is the leavers’ revocation process?	Upon resignation, an employee’s badge is collected by Human Resources and deactivated within the hour by Facilities.

Logical Security Controls

User Authentication

All users should be authenticated before they can gain access, to ensure that only authorized users gain access to any information or systems within the computer installation.

Criteria	Response
How is authentication performed?	Login to the Angel.com production network is done via SSH tunneling with two-factor VPN challenge.
How is access granted?	Access is granted when the user can enter a valid personal username, password, and random generated identifier from VPN dongle.
Who establishes access criteria?	Director, Data Center Operations.
How is information confidentiality protected?	Usernames and passwords are personal, secret, must meet strong password criteria, and are revoked upon termination. The password policy meets PCI compliance requirements.

Monitoring

Logs of all key events within the computer installation should be maintained, reviewed periodically, and protected against unauthorized change, to ensure individual accountability and to enable incidents, such as access violations, to be investigated and resolved.

Criteria	Response
How are occupants monitored?	Via closed-circuit camera installation and recording equipment, via access, audit, and application event logs.
What logging is performed?	Security logs, access logs, and application logs on each host and network device.
How are logs stored?	Logs are stored centrally in a monitoring server via syslog protocol.
What is the log retention period?	Logs are backed up in a 1-year rotation policy.
What network monitoring devices are installed?	IDS, Vulnerability Scanner.
How is wireless networking controlled?	We use no wireless networks.
How are onsite external network connections managed?	Via VPN concentrator.

Device Security Management

Patch Management

Criteria	Response
What procedures are in place for managing application of operating system and application patches?	For DMZ hosts, we follow the PCI Authorized Scanning Vendor policy; we must pass these scans on a quarterly basis. For hosts inside of the DMZ we follow a biweekly operating system patching policy.
What procedures are in place for monitoring patch status of networked devices?	Vulnerability Scanner.

Virus Monitoring

Criteria	Response
What procedures are in place for managing application of virus signatures of networked devices?	We use a Symantec central virus server that distributes virus signature files to the virus scanners installed on each host. These virus definitions are distributed every 24 hours.