Security Plan

In the event that **US Internet** makes material changes to practices, policies, processes and/or procedures, your company should be notified immediately. Your company has the right to review all plans, processes and procedures mentioned here with scope limited to your company projects executed by **US Internet**. **US Internet** is in compliance with resident government's requirement on all licenses and legal registrations.

Security Consideration	***Requirements***	***Standards/Specifications***	***US Internet Response***
Security Services	State-of-the-art security products and services to protect any computer system or network device to provide services against the risk of penetration by or exposure to a third party.	• Protection against physical intrusions • Protection against intrusions of operating systems or software • Encryption of confidential information • Securing the computer systems and network devices • Well defined security policies and practices • Use of strong encryption techniques such as Public/Private keys, Digital Signatures, Virtual Private Networks, and Digital certificates. • Specify all licenses and legal registrations required for offshore electronic processing as dictated by the resident government are in place and up-to-date. • Immediate notification of any material changes to practices, policies, processes and/or procedures. • Right to review all plans, processes and procedures mentioned herein.	• 24 X 7 Monitoring by recorded video surveillance and operation is manned 24/7. • Well defined security policies and practices in place • Strong encryption techniques are being used such as 3DES.
Personnel Policies & Practices	Employees, agents or representatives assigned to perform services shall have the proper skill, training and background so as to be able to perform in a competent, timely and professional manner and all work will be so performed.	• Background checks, using a recognized company, including but not limited to criminal and credit checks, for individuals in key roles • Exit interviews on terminating employees (to include recovery of portable computers, telephones, smart cards, equipment, keys, identification badges) • Employees, agents or representatives assigned to perform Security Hosting Services shall be bonded.	• HR has process for background checks for individuals in key roles. • Process in place to recover assets from terminated employees • Every employee signs a non-disclosure and confidentiality agreement

Security Plan

		• Non-Disclosure and Confidentiality Agreements required for all vendor assigned staff	
Your company Audits	Allow Your company to conduct audits on third party and/or its affiliate third parties to determine level of compliance with all security standards and specifications pertinent to the product(s) and/or service(s) being provided.	<u>Audits may include but not be limited to:</u> • Vulnerability assessments (Remote & On-site) • Penetration tests • Review of any and all system, network, application or security logs • Interviews with vendor employees or other vendor affiliates • Observation of day-to-day operations • On-site inspections of the hosting facility	• Observations, interviews, inspections can be done with sufficient advance notice. • If available, an executive summary of the most recent third party Vulnerability Assessment Report will be made available to your company upon request.
Third party to Affiliate Third party Audits	Third party will conduct audits to determine level of compliance with all security standards and specifications of Affiliate Third Parties as set forth by Your company.	<u>Audits may include but not be limited to:</u> • Vulnerability assessments (Remote & On-site) • Penetration tests • Review of any and all system, network, application or security logs • Interviews with vendor employees or other vendor affiliates • Observation of day-to-day operations • On-site inspections of the hosting facility	• Audits will only be allowed by your company staff with sufficient advance notice.
Operational Processes	Perform operational processes as reasonably requested by Your company.	• Monitor, audit, and test systems and networks for possible security problems on a regular schedule (e.g. vulnerability assessments, network penetration testing) • Review security logs daily and investigate anomalies as needed • Test, install, and maintain security infrastructure tools and vendor products	• Monitoring is done on continuous basis, internal audits are done every 3 months. • Well equipped security infrastructure with tools and vendor supplied products is in place. These tools include Nessus
Physical Security	Adequate physical security measures and practices to secure and maintain a network operation center.	<u>Security Controls</u>: • Security components should include access restrictions, interior and exterior video surveillance, security guards, video monitoring, closed circuit TV, motion detectors, gates, locks, secure key cards, alarms, personal ID cards and biometric controls	• Video Monitoring systems in place in datacenter, inside and outside of building • Customer equipment kept in locked racks, only USI techs have keys • Datacenter door secured by biometric

		• 24x7x365 Security Staff • Systems isolated both physically and logically from any other systems • Monitor network anomalies <u>Environment Controls</u>: • Uninterruptible power supply ("UPS") and a back-up generator for all Equipment. • Appropriate air-conditioned environment (between 60 degrees and 78 degrees Fahrenheit) and proper humidity level (between 45% and 55%) for the equipment. • A water-free fire suppression system. <u>Process Controls</u>: • Non Authorized Personnel/Visitor Logging • Regular review of Non Authorized Personnel/Visitor access logs • Process to ensure terminated employees/consultants/guards surrender all identification, keys and access cards before they depart from premise • Process for access card de-activation within 24 hours of notification. • Periodic audit of card system • Documents not discarded in whole, readable form are shredded, burned, or otherwise mutilated	system and keypad • Network anomalies are monitored through alert software and log reviews. • All visits are logged including those of non-authorized personnel. • Redundant Liebert UPS and air-conditioning in place • Ana-laser fire suppression in place
Network Security	Minimal deployment of the following baseline controls on all network devices.	• Use of login Banners at login time • Network traffic filters and Access Control Lists to restrict unauthorized traffic • Strong authentication mechanisms for all console or remote administrative access • Firewalls to permit only authorized traffic • Controls to ensure the integrity and confidentiality of the appropriate Domain Name Server data • Use of network based intrusion detection tools • Use of digital certificate verification between server/sever and server/client • Use of Virtual Private Networks or equivalent	• Login Banners used • Filters and access control filters are in place • Firewalls permit only authorized traffic • Network based intrusion detection • Strong authentication mechanisms in place for all types of access. • Radius and TACACS+ for authentication

Security Plan

Anti-Virus	Maintain anti-virus measures	• Host and Web based • Inbound and outbound monitoring on all data transfer mechanisms and all e-mail systems • Early virus alert service from vendors • Real-time on-line access scanning • Timely updates to signature files and search engines	• Host-based Anti-virus on servers and desktops • Virus signatures updated frequently • Real-time scanning • Symantec Antivirus Corporate edition • Email scanned by McAfee, F-Prot, Kaspersky anti-virus
Host Server Security	Deployment of baseline controls on all host servers including detail description of operating/file system controls used to secure servers and access controls (authentication & authorization) on servers, platforms, and databases	• Review all default settings • Strong access control lists to restrict unauthorized access • Remove unneeded network protocols, default or system user accounts, and any sample application code • Resetting of default passwords (includes periodic password resets) • Use of dedicated servers as required • Use of partitioned servers are available as needed • Other measures as recommended by the OS vendor	• ACLs in place to restrict access • Unneeded network protocols, user accounts, and sample application code removed • Use of dedicated servers • IIS lockdown tool • Security templates • Security checklists • Group policies • Default Passwords reset and changed periodically
Identification, Authentication and Authorization.	Restrict electronic access to the Your company Site beyond customer-level access to only authorized persons.	<u>Security Controls</u>: • Clients are uniquely identified and authenticated by your company site systems. ***The use of any form of generic or shared user identifier is expressly prohibited.*** • Client-level access enforce by the "least privilege" principle (i.e. Clients *only* have the level of access to the system required to perform their job functions.) • Strong, industry standard encryption technology (e.g. in 2000, 3DES or Blowfish) to encrypt all data identified by your company as "sensitive" or "confidential". • Use of tools to remove all Client data and data identified as "sensitive" or "confidential" from any media, whether magnetic, optical or any other form, before disposing of such media.	• Clients uniquely identified • Default passwords are reset and changed • Password files encrypted and secured • Access limited to only what is needed • US Internet forces strong passwords for all accounts

Security Plan

		Management of Passwords: • Passwords changed at least every 45 days • Default passwords changed immediately upon account creation • Password file must be encrypted and secured • Ten (10) unique passwords within a password history cycle • Password length at least 6 characters • Use of strong password structure (Ex: "Pa33WorDS") • Password measures enforced automatically Management of User Accounts: • User accounts and passwords audited every 90 days for compliance • Accounts disabled or locked after 3 failed login attempts within a 30-minute period. • Locked accounts re-enabled by authorized system or security administrator • Verification information for resetting passwords selected by Client • Time-out feature for inactivity • Inactive user accounts purged after 90 days	
Data Transmission Security	Safeguard the confidentiality and integrity of all Your company or Client data being transmitted over any form of data network.	• Strong, industry standard encryption for Client data or other data identified as "sensitive" or "confidential. (Examples include SSL for Web browser sessions, or PGP file encryption for bulk data transfers.). • Strong, industry standard session encryption for administrator, root or super-user access to a Your company Site system from some other system. (Ex: Secure Shell ("SSH")) • Secure Socket Layer ("SSL") or stronger encryption techniques for network access via the public Internet. • Strong industry standard tools for monitoring, controlling, and administering electronic transmissions.	• Strong encryption in use such as SSL • Debug logging is enabled in firewalls • SSH in use for administrator access
Data Security	Safeguard the confidentiality and	• Data level encryption	• 3DES encryption used

(Production & test)	integrity of all Your company or Client data stored and maintained at the vendor site.	• File integrity protection tools	
Firewall Services	Use of firewall tools and services in accordance with Your company's requirements, policies and procedures, including general maintenance and monitoring of firewalls and implementation of firewall rule set changes.	• Controlled implementation and scheduled maintenance of firewall rule set changes • Active monitoring to identify attempted or actual security violations • Controlled emergency maintenance of firewall rule set changes • Two (2) business day turnaround time for firewall rule set changes	• Active Monitoring of firewall logs • Emergency maintenance done after getting approval • 2 day turnaround for firewall changes
Intrusion Detection Services	Use of intrusion detection tools to detect unauthorized access to or unauthorized activity on the networks, computer systems and network devices associated with the Your company site.	• Network and/or Host based • Active monitoring to identify attempted or actual intrusions • Timely updates to signature files	• Network based IDS in place • IDS alerts monitored actively • Logs monitored to detect intrusion • Timely updates are made
Backups and Other Media Handling	Availability of all Your company site systems and Client data by using standard data replication tools and methodologies such as total redundancy between multiple sites, disk mirroring, data stripping, or electronic vaulting to a separate geographical site.	<u>Operational Backups:</u> • Full backups performed once per week • Incremental or differential backups performed once per day • Two (2) month rotation of full backups on-site • Tapes duplicated once per week and then moved to an offsite location • One (1) full month of incremental backup tapes retained on-site. • Four (4) hour restoration limit <u>Other Media handling:</u> Policy and process for ensuring appropriate procedures are implemented, maintained and monitored to protect documents, computer media, input/output data and system documentation from damage, theft and unauthorized access. Policy and process to include: • Management of removable computer media (e.g. tapes, disks, cassettes, printed reports) • Disposal of media	• Full backups are performed once per week • Incremental backups are done every day. • Off-site location is used for all development centers. • All the media are destroyed before disposal.

Security Plan

		• Information handling procedures • Security of system documentation	
Disaster Recovery	Your company shall reasonably determine the level of resumption of Your company Site services.	• A Current and audited executable Disaster Recovery Plan. • Frequency and duration of Disaster recovery exercises	• A DRP is designed and in place and is available for review at customers request.
Business Continuity Management	Contingency plans must be implemented to ensure that essential business processes can be restored within the required time period.	• Regular plan testing using a variety of techniques such as table-top testing of various scenarios, simulations, technical recovery testing, testing recovery at alternate site, tests of supplier facilities and services, and full scale compete rehearsals • Plans maintained by regular reviews and updates to ensure their continuing effectiveness • Maintain a documented continuity strategy consistent with the agreed business objectives and priorities • Maintain a documented business plan consistent with the agreed strategy • Maintain a Business Continuity Planning Framework that includes conditions for activating plans, emergency procedures describing actions to be taken following incident, fallback procedures for moving to alternative temporary locations, resumption procedures, maintenance schedule for plan updates and testing, awareness and education activities, and individual roles and responsibilities.	• BCM plan includes off site backup, of environment and equipment to assure future uptime for clients in the case of catastrophic failure.
Security Monitoring	Provide monitoring services.	• Real time monitoring of all systems and network devices/systems to detect potential security violations. Such monitoring will include but is not limited to operating system access, detection of unauthorized processes or software, unauthorized modification of existing software or data, or unauthorized configuration changes to computer systems and network devices. It will also include the logs of all firewalls, intrusion detection systems,	• Alerts enabled on network devices and firewall. Logs are reviewed to identify violations • Logs stored in syslog server • Logs retained for future purposes

Security Plan

		physical access controls, or other security-related systems. • Retain the logs of all security-related systems, to include but not limited to firewalls, intrusion detection systems, access control measures (both electronic and physical), and file integrity checker logs for forensic or evidentiary purposes.	
Incident Response	Reporting of any and all security incidents.	• Security Incident Response Plan acceptable to Your company • Log of security incidents must be maintained and classified as confidential and proprietary property of Your company • Incident Report and Action Plan per incident	• We have incident reporting procedures and policy in place. • Incidents are followed under the US Internet Escalation procedure and escalated on Varity of incident.
Information Confidentiality	Safeguard the confidentiality and integrity of all Your company information.	• Use prudent disposal methods that will prevent further distribution • Must meet requirements and other restrictions as may be imposed by law • Maintain the confidential nature of the information and appropriate restrictions on use and disclosure	• We have non-disclosure agreement with associates and third parties. • We use a shredder for destroying confidential documents.
Configuration Control and Change management.	Formal procedures to manage changes to the computing environment	• A Current and audited executable Change Configuration management Process	• All changes are documented and authorized by senior management and ticketed under Team Builder are internal ticketing and call log software.
Web Security Controls	Measures to protect company defined web sites.	• Web servers with public content installed on separate network protected by a firewall (DMZ) • Web monitoring and reporting	• Does not pertain to existing service

Security Plan

Remote Access	Measures to restrict remote electronic access to the Your company Site beyond customer-level access to only authorized persons.	• Strong remote session encryption (e.g. IPsec, F-Srcure VPN+, PowerVPN) • Logging of access connection and attempts • Strong identification and authentication tools (e.g. SecureId)	• IPSec is used for all remote sessions. • RADIUS authentication server is deployed. • TACACS+ authentication server is deployed • RADIUS authentication server is deployed • All access attempts logged
Asset Management	All major information assets must be accounted for and have assigned ownership.	Policy and process for ensuring asset management requirements are implemented, maintained and monitored. Policy and plan to include: • Inventory of important assets including the relative value and importance of asset • Assigned responsibility for maintenance and implementation of appropriate controls. • Assignment of each asset with the appropriate security classification (e.g. application software, data files, databases, system documentation, continuity plans, laptops, fax machines, etc.) • A documented classification system defining an appropriate set of protection levels and handling measures (e.g. how assets are to be handled and protected)	• All assets are owned, maintained and managed by US Internet Corp.
Application Development and Maintenance	Security within applications	Policy and process for ensuring application security requirements are implemented, maintained and monitored. Policy and plan to include: • Input data validation • Security controls in application processing • Message authentication • Output data validation • Protection of test data • Access control to software libraries • Change control processes and signoffs by IP • Process and restrictions on software installations and upgrades • Management of outsourced software	• Security in place for secure code changes, updates and new implementations. • All changes are signed off by management before implemented into environment.

Security Plan

		development	
Data Privacy	Safeguard the confidentiality and integrity of data privacy of Your company system users and customers., particularly for personally identifiable information	• Policy and process concerning of data privacy for data including personally identifiable information for Your company users, clients, affiliates and customers that is accessed or hosted by a third party that assures protection and the compliance with laws and legal statutes. • Escalation process to notify Your company when product(s) or service(s) are found to be in violation of compliance requirements • Reviews and audits for legal compliance • Action plans for establishing compliance	• There is a well-defined process in place to maintain confidentiality of customer data. • Escalation process for notifying your company needs to be established and will be completed by Your company and IBM and provided to US Internet to fulfill. • Periodic reviews and audits are done. • Action plans are devised if there is non-compliance
Legal Compliance	Process to ensure use of product(s) and/or provision of services are in compliance with legal requirements	• Policy and process concerning of Your company confidential data and intellectual property rights that is accessed or hosted by a third party that assures protection and the compliance with laws and legal statutes. • Escalation process to notify Your company when product(s) or service(s) are found to be in violation of compliance requirements • Reviews and audits for legal compliance • Action plans for establishing compliance	• Governed by Consultant Engagement Agreement dated May 15, 2003
Security Escalation Process	Escalation process with criteria and contact information between Your company, and the third party for the purposes of notification and actions required concerning security incidents.	• Escalation plan acceptable to Your company • Log = security incident log for formal documentation • Reporting and action plan: = Security Incident Plan per incident.	• Escalation provided to US Internet by your company. • Governed by Consultant Engagement Agreement dated May 15, 2003