Securence Security and Compliance Supplemental

This document is supplied as a supplemental to the US Internet **Operational Controls and Procedures** document as a clarification of security measures specific to the Securence solution. The **Operational Controls and Procedures document** is the defining control document and outlines all aspects of US Internet's control procedures. The sections of this document are excerpts from the **Operational Controls and Procedures** document. Detailed information and full controls can be found within the **Operational Controls and Procedures** document.

Risk Assessment

US Internet has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable transaction processing for user organizations. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks. Risks that are considered during managements risk assessment activities include consideration of the following events:

- Changes in operating environment
- New personnel
- New or revamped information systems
- Rapid growth
- New technology
- New business models, products, or activities
- Corporate restructurings
- Expanded operations
- New accounting pronouncements

Security Principles

US Internet has built the Securence solution with the highest level of data protection in mind. With millions of dollars in online transactions a day, US Internet has, over the past 15 years, developed a data protection policy that surpasses the strict PCI compliance requirements. We then utilized this expertise and deployed the time tested PCI standards as the baseline of the Securence solution. By augmenting these procedures based on specific requirements of other industry standard regulations we provide a level of data protection not easily matched. As part of the US Internet family of service offerings, the Securence policies and procedures have been rigorously tested and audited as part of our SAS 70 Type II certification. A brief outline of the PCI methodology and specific US Internet implementation follows:

Build and Maintain a Secure Network

Utilizing state-of-the-art firewall technologies and enforcing strict internal controls including server build, configuration, and access control standards US Internet has designed and built our Securence system with security foremost in our minds. That infrastructure is then deployed in our state-of-the-art datacenter facilities. The US Internet datacenter facilities have been constructed with the British Security Standard (BSS) as the baseline. This standard is more stringent than the more often used industry standard Grim Leach Bliley (GLB) standards. These features, in combination with a rigorously

enforced access control policies for both physical and logical network resources allows US Internet to maintain a highly secure network environment.

Protect User Data

User data, as it applies to message form, is most susceptible during three phases of it's lifecycle; Reception, Storage and Transmission. US Internet has gone to great lengths to mitigate the risks associated with each of these phases and provides a level of data protection above common industry standards.

Reception:

While no entity has the ability to enforce security standards on outside third parties transmitting messages containing sensitive or confidential information without appropriate encryption or other protective measures, the Securence solution provides mechanisms that can limit sensitive data exposure through the enforcement of connection specific security requirements. Those restrictions are accomplished through the use of the industry standard Transport Layer Security (TLS) protocols. All Securence servers are configured by default to utilize TLS. During the negotiation process between the transmitting outside mail server and the receiving Securence sever the transmitting server is informed that TLS in enabled on the receiving server. If properly enabled, and utilizing one of the approved FIPS 140-2 cipher suites, the transmitting server will utilize TLS to form a secure tunnel between the two servers safeguarding the message payload. By default, unknown mail servers that choose not to employ TLS will still have their message accepted. In the event the transmitting mail server is known to the Securence system (a message partner) such as a State agency, the connection can be configured to require TLS or the message will be refused and the connection will terminated. Message partners can be identified through Domain, IP address or individual email address.

Storage:

The Securence solution provides two disaster recover features; Shadow and Archive. These features provide a means by which messages that have been processed can be retrieved for up to 10 years after delivery. To accomplish this functionality US Internet is required to store a secured copy of every message. To protect the security of any information contained within a message US Internet employs AES 256 encryption in CTR block cipher mode. Access to the key store containing the decryption cipher is restricted to a few key trusted employees at US Internet.

Transmission:

Transmission allows for the greatest control over message delivery handling options. Through the creation of message partners US Internet can require that all servers Securence is delivering messages to utilize TLS configured to use the highest levels of FIPS 140-2 cipher suites. In this instance all message delivery should be to designated State mail system servers and the State's system should never by accepting mail from any source outside of the Securence solution. As such, the State has the ability to create a rule set denying any mail from a source outside os Securence greatly increasing the security level of the state's electronic message systems.

US Internet has taken additional steps to provide an even greater level of user data protection with its CypherMail solution. This solution provides the greatest level of data protection in the form of true message payload encryption. When utilized, the entire message body is encrypted utilizing AES 256 in CTR block cipher mode from end to end without the need for any additional software or client being installed on either the sender or receivers computer.

CypherMail:
We developed CypherMail to enable secure delivery to any destination independent of transport methods used. In addition to the safeguards utilized above for Reception and Transmission, Securence can be configured to deliver the final step using CypherMail.

When a message requires CypherMail the following steps happen:

1. A secure random key and initialization vector is generated using true entropy sources.
2. The original message is encrypted using AES 256 in CTR block cipher mode.
3. The encrypted message is inserted into an HTML document and then into a new email.
4. The original message is deleted.
5. The new message containing an HTML file is delivered to the recipient.

When the recipient receives the message the following steps happen:

1. The recipient is prompted to open the attached HTML file in their web browser.
2. The full encrypted message is sent from the recipient's computer to the Securence web server.
3. If the recipient doesn't have an account they are prompted to create a new account with a second email for verification.
4. The user is authenticated.
5. The message is verified against available viewing times, number of views and revocation options that the original sender has selected.
6. The decryption key is retrieved from our key store.
7. The message is decrypted and presented to the user within the web interface.
8. If the original sender has selected notification, an email message is generated notifying the original sender that the message has been read.
9. The recipient may download attachments.

Within the CypherMail interface the recipient may reply to the message or forward the message providing the original sender allows these actions.

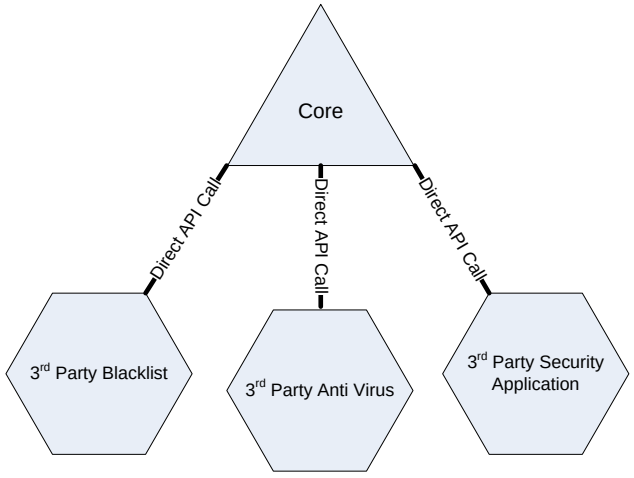
Maintain a Vulnerability Management Program

US Internet's Vulnerability Management Program addresses vulnerability in two classifications; Dependency Prevention and Ongoing Risk Assessment.

Dependency Prevention:

At the foundation of the Securence solution is the early identification of the potential risk of dependency due to reliance on third party components within the core coding of our solution. To completely mitigate that risk US internet made the decision to completely self-develop our solution. As such US Internet owns 100% of the base coding. This decision has given US Internet a competitive advantage. With a dedicated on-site development team US Internet has the ability to make unrestricted modifications to the core code to accommodate the requests of our client base, mitigate newly identifies risks as they arise and respond to global message storms with unequaled speed and efficiency

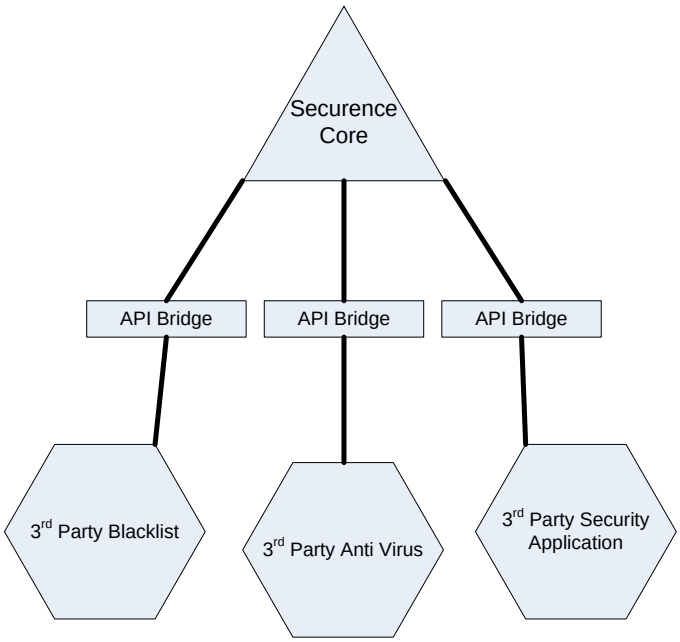
Recognizing that 3rd party application can provide additional functionality, our development team created a unique coding configuration utilizing API "bridges" to incorporate virtually any 3rd party application as functionality of the Securence solution. This design provides an insulating intermediary between the base core code of Securence and the 3rd party application. In a traditional solution the core code itself would call that functionality directly as seen in the diagram below.



Our staff identified this as a potential risk as it requires changing of the core programming for the addition, modification or removal of any additional 3rd party application functionality. Any change to the core to accommodate a 3rd party application carries potential risk as it may require changes that have cascading and/or unforeseen impact on critical components and/or functionality.

Securence has been constructed to be completely modular. A custom API bridge is created for each 3rd party application. This allows for the addition of any functionality provided by that program to the Securence solution as a feature while isolating the impact of any change to the

3rd party application only. Any 3rd party change, addition, or removal, requires modification of the bridge only, the base core code remains unchanged.



Ongoing Risk Assessment:

Ongoing Risks are classified as either internal or external.

Internal:

As previously mentioned, any change to the base core code of a program carries inherent risk. To mitigate that risk US Internet has implemented a tiered code review process. At the heart of that process is an isolated production mirrored development environment. Duplicating all production functionality within that environment, our development staff has the ability to stringently test all potential code variation in real-time. Following a ten step process our development team has created a procedure to mitigate risk associated with even a minor code change.

1. Change requirement identified through product review and customer request
2. Initial code development
3. Deployment within development environment
4. Analysis of code effectiveness
5. Revision of code as required
6. Submission to QA for review
7. 24 hour burn in within development environment (non-emergency response change only)
8. Submission to Senior Developer for approval
9. Deployment in production environment
10. Post mortem analysis

External:

External vulnerabilities include unauthorized access to physical and /or logical resources, malicious attach (spam storm, virus release, etc…), vendor services failure, or any other event outside of the direct control of US Internet. To mitigate these risks US Internet constantly monitors global message events, server load statistics, world network health as well as ensure constant updating of all spam filters, virus definitions, and malicious content databases. We also utilize the "bridged API" model as mentioned in the Dependency Prevention response above. As well as ensuring that all infrastructure is n+1 redundant at a minimum. For a detailed explanation please see attachment A, Facilities, Security, Response Management and Change Control Document.

Enforce Strong Access Control Measures

US Internet has developed a documented Access Control Policy that ensures the security and integrity of all physical and logical network resources. That policy is constantly reviewed and updated as potential risks are identified through the risk assessment procedures developed as part of our Vulnerability Management Program. The control measure put in place are then subjected to rigorous internal auditing processes and further validated by outside auditors during our yearly SSAE 16 SOC 1 audit. A copy of our **Operational Controls and Procedures** can be obtained under NDA.

Regularly Monitor and Test Networks

All aspects of the US Internet network are continuously monitored 24 x 7 x 367 both electronically and by live personnel. Our state-of-the-art facilities are manned 24 x 7 x 365 with staff conducting hourly walkthroughs of the facility to validate that all physical and environmental security measures are in place and functioning correctly. In addition US Internet employs multiple electronic monitoring devices that provides immediate notification should any condition exist that is outside of set thresholds.

US Internet has a dedicated Security Specialist that monitors our network to identify unauthorized access attempts or potential vulnerabilities. Those tasks include periodic review of biometric access logs for unauthorized access attempts, intrusion testing of network devices, bandwidth and server resource utilization monitoring, and more.

Maintain an Information Security policy

US Internet has developed extensive documentation and policies that ensures the security and integrity of all physical and logical network resources. That policy is constantly reviewed and updated as potential risks are identified through the risk assessment procedures developed as part of our **Operational Controls and Procedures**. The control measure put in place are then subjected to rigorous internal auditing processes and further validated by outside auditors during our yearly SAE 16 SOC 1 audit. A copy of our **Operational Controls and Procedures** can be obtained under NDA.

Compliance

HIPAA:

The described above procedures provide the highest level of protection and meet or exceed the requirements for safeguarding of personally identifiable medical records in keeping with the HIPAA standards.

IRS publication 1075

The described above procedures provide the highest level of protection and meet or exceed the requirements for safeguarding and protecting tax returns and tax return information in keeping with the IRS Publication 1075 " *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities".*

FIPS 140-2

The described above procedures for reception, storage and transmission of messages details the requirement for FIPS 140-2 certified encryption algorithms for TLS connections with the Securence system. To ensure the highest level of security we do not support any FIPS 140-2 cipher suite encryption weaker than 3DES. The following TLS cipher suites are utilized within our solution:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

In addition, CypherMail utilizes AES 256 in CTR block cipher mode.

NIST 800-45

The NIST Special Publication 800-25 details guidelines for Electronic Mail Security. Due to the volume of mail processed (**in excess of 200 Million messages a day**) the US Internet Mail environment and specifically the Securence AS/AV solution set have been developed to exceed the recommendations of this publication.

FERPA Regulations

The described above procedures provide the highest level of protection and meet or exceed the requirements for safeguarding of Student records as described in the Family Educational Rights and Privacy Act.

CJIS

US Internet recommends the highest of the Securence security configurations. The feature sets this configuration enables allow for our system to surpass the recommended minimums for message security.

NC Statewide Security Standards

Utilization of FIPS 140-2 suites, TLS connection tunnels, as well as our own internal strict access and control procedures, allow our Securence solution to meet, or exceed in most cases, the recommendations and requirements of the NC State Security Standards.