SOC 3 for Security, Availability, Processing Integrity, and Confidentiality

Independent Practioner's Trust Services Report

For the Period November 1, 2016 through October 31, 2017

Independent SOC 3 Report for the Security, Availability, Processing Integrity, and Confidentiality Trust Principles for Zix Corporation

ZIX CORPORATION

INDEPENDENT PRACTIONER'S TRUST SERVICES REPORT – SOC 3

Table of Contents

SECTION ONE: INDEPENDENT PRACTIONER'S TRUST SERVICES REPORT

To the Management of Zix Corporation:

Scope

We have examined management's assertion that during the period November 1, 2016 through October 31, 2017, ZixCorp (the "Company") maintained effective controls over its ZixPort, ZixONE, and Hosted Services system, based on the American Institute of Public Accountants ("AICPA") and Chartered Professional Accountants of Canada ("CPA Canada") trust services security, availability, processing integrity, and confidentiality criteria to provide reasonable assurance that:

- the system is protected against unauthorized access, use, or modification);
- the system is available for operation and use as committed or agreed;
- the system processing is complete, valid, accurate, timely, and authorized; and
- the system information designated as confidential is protected as committed or agreed.

The Company is responsible for this assertion. Our responsibility is to express an opinion based on our examination. The Company's management description of the aspects of the ZixPort, ZixONE, and Hosted Services system covered by their respective assertion is outlined within the report.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of the Company's relevant controls over security, availability, processing integrity, and confidentiality of the ZixPort, ZixONE, and Hosted Services system; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary during our examination. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, the Company's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct errors or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, the Company's assertion referred to above are fairly stated, in all material respects, based on the AICPA and CPA Canada trust services security, availability, processing integrity, and confidentiality criteria.

ZixCorp's use of the AICPA Service Organization logo constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to update this report or provide any additional assurance.

CyberGuard Compliance, LLP

November 28, 2017

Orange, California

SECTION TWO: ZIXCORP'S ASSERTION REGARDING ITS ZIXPORT, ZIXONE, AND HOSTED SERVICES SYSTEM

November 28, 2017

During the period November 1, 2016 through October 31, 2017, the Company, in all material respects maintained effective controls over the ZixPort, ZixONE, and Hosted Services system, as defined by the 'System Description' attached within the report, to provide reasonable assurance that:

- The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.
- The system is available for operation and use to meet the entity's commitments and system requirements.
- System processing is complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements.
- Information designated as confidential is protected to meet the entity's commitments and system requirements

Further, the Company confirms that to the best of our knowledge and belief, that the controls related to the trust services security, availability, processing integrity, and confidentiality criteria were suitably designed and operating effectively during the period November 1, 2016 through October 31, 2017, to achieve those control objectives. The criteria we used in making this assertion were that:

- The risks that threaten the achievement of the controls related to the trust services criteria have been identified by the Company; and

- The controls related to the trust services criteria would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the trust services criteria from being achieved.

ZixCorp

SECTION THREE: DESCRIPTION OF ZIXCORP'S SYSTEM

OVERVIEW OF ZIXCORP'S OPERATIONS

ZixCorp operations are conducted from the corporate office located at 2711 North Haskell Avenue, Suite 2200 LB36, Dallas, Texas, 75204. Operations at this location include security, availability process integrity and confidentiality. ZixCorp provides email encryption services for privacy and regulatory compliance with over 56 million protected email recipients including encrypted email delivery to healthcare organizations, financial institutions and government agencies. ZixCorp supports five encrypted email delivery mechanisms including S/MIME, TLS, OpenPGP, secure portal and "push" delivery.

Description of ZixData Center℠

ZixData Center℠, located in Dallas, Texas with a backup facility in Austin, Texas, has the capacity, scalability and infrastructure to support encryption keys for every email address in the world. *ZixData Center* is staffed 24-hours a day with operations personnel monitoring the facilities, networks, systems and applications. The physical security of the *ZixData Center* employs a five-layer security approach. Access to the *ZixData Center* is controlled through a series of doors that employ access controls such as 24-hour security guards, electronic badge readers and biometric devices used in combination with a badge reader. Operations staff has been carefully screened, including background checks performed by an external investigation firm.

Uninterrupted electrical power is required for the continuous operation of servers, communication equipment and environmental controls. ZixCorp's policy of complete redundancy has been designed to ensure there are no potential single points of failure throughout the data center for any given system component. Two independent high-bandwidth fiber trunks move traffic in and out of the data center to mmultiple and redundant internet service providers.

ZixData Center Key Benefits:

- Redundant electrical feeds from independent utility power grids
- Redundantly configured fiber connections and redundant routers
- Dual uninterruptible power supplies
- Sun Microsystems Solaris-based systems and Intel Linux-based systems
- Back-up diesel generator
- Scalable web server architecture
- Redundantly configured power distribution units
- 99.99% reliability
- Multiple ISPs

Description of ZixCorp Services - BYOD

ZixOne[SM]

ZixOne is the Bring Your Own Device (BYOD) solution that bridges the gap between enterprise security and expense concerns and the growing preference among employees to maintain a single mobile device for office and personal use. For organizations, ZixOne satisfies security requirements by allowing organizations to keep their data stored on their servers and control employee access. ZixOne eliminates the need for organizations to purchase, maintain and issue mobile devices or services to employees. It also significantly reduces legal exposure to privacy issues. For employees, ZixOne offers the ability to manage both personal and enterprise data on a single mobile device without losing convenience, control or privacy with their personal mobile devices. Employees can choose from a variety of IOS® or Android™ mobile devices.

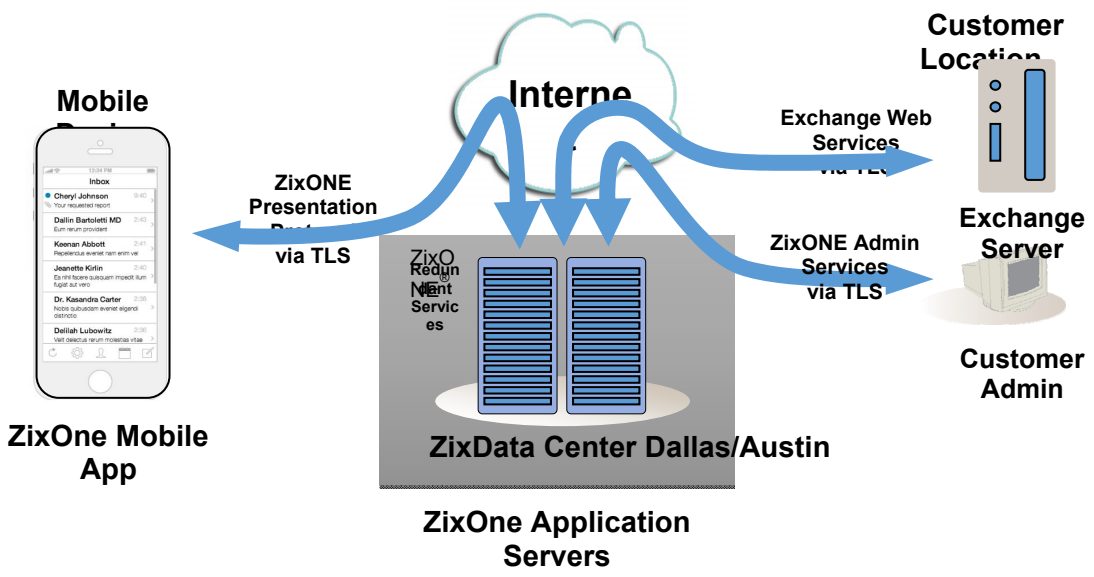
Organization administrators can immediately suspend mobile device access to the ZixOne server using the browser- based Administration Console. Administrators can use the Administration Console to limit ZixOne usage to an exclusive access list. Searchable mobile device activity logs on the console's Reports screen give administrators monitoring and diagnostic capabilities as well.

ZixONE Key Benefits:

- No corporate data stored on the device
- Simple, secure connection to the office
- Seamless user experience
- Employee privacy and control
- Per user pricing

ZixONE Key Features:

- Android and iOS compatible
- High-efficiency protocols deliver data quickly and securely
- Easy administration controls for disabling access
- Reporting capabilities for improved regulatory compliance



Description of ZixCorp Services – Email Data Loss Prevention

ZixQuarantine

Email is the most used communication tool in business. It enables organizations to conveniently collaborate and share valuable information, from customer data to intellectual property, inside and outside an organization's network. With ZixDLP, an email data loss prevention tool, your organization can monitor and protect the channel that both assists your company in running efficiently and exposes your organization to the most risk. Leveraging ZixCorp's leadership and expertise in email encryption, ZixDLP combines our proven policy and content scanning capabilities with an intuitive quarantine interface. ZixDLP provides you with the ability to:

- Use ZixGateway policies to quarantine email that contains sensitive information.
- Scan outbound email messages for violations based on sender, recipient, subject, body and attachments using lexicons, file types and other filters.
- Process quarantined email messages by:
- Creating authorized users who can process quarantined messages.
- Reviewing policy and content violations for a quarantined message.
- Searching and filtering messages, assigning category labels and applying comments.
- Releasing and deleting multiple quarantined messages concurrently.
- Sending notification messages to employees regarding quarantined emails.
- Review quarantine reports using the ZixReporting Dashboard.

ZixQuarantine Key Benefits:

- Easy to use and cost-effective
- Enhanced visibility into sensitive information in outbound email
- Strengthened compliance with corporate policies
- Improved employee education regarding the treatment of sensitive information

ZixQuarantine Key Features:

- Powerful administrative capabilities
- Intuitive administrative dashboard
- Reporting of quarantine activities and trends
- Deployable as a bundled, ad-on or standalone solution

Description of ZixCorp Services – Email Encryption

*ZixGateway*SM

ZixGateway is a policy-based email encryption service that uses an appliance for enterprise-wide regulatory compliance. It provides company-wide security, content filtering, and management of outbound corporate email. *ZixGateway* provides the benefits of a secure messaging gateway without having to create and manage encryption keys, by leveraging the email encryption directory, *ZixDirectory*. Plus, it is totally transparent to end users.

ZixGateway enables organizations to comply with industry regulations and corporate security policies with built-in lexicons that automatically encrypt messages to meet specific needs including healthcare, finance, and profanity. *ZixGateway* provides a secure and private channel for email communications between employees, customers, and business partners — or anyone with an email address. *ZixGateway* employs efficient and secure ways to deliver messages through ZixCorp's unique *Best Method of Delivery*.

Superior support for TLS

The latest version of ZixGateway also offers unique support for TLS in several ways. TLS through ZixGateway provides:

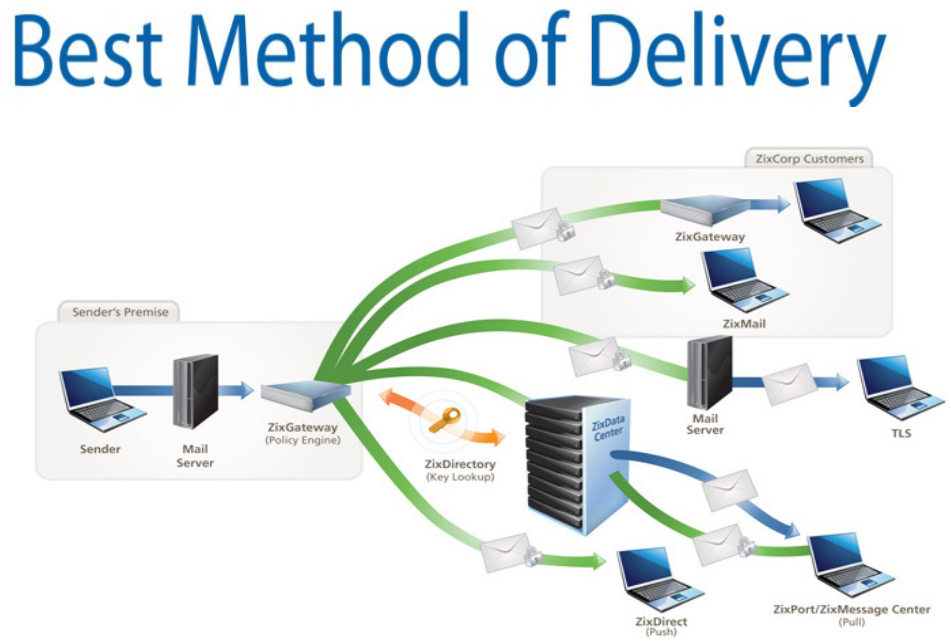
- Secure, bidirectional transparency - ZixCorp Best Method of Delivery chooses the most secure and transparent delivery method available for each message. ZixCorp S/MIME provides high security and bidirectional transparency. If S/MIME is not available, TLS can be configured as an alternative transparent delivery method.
- Simplified set-up of mandatory TLS - By making TLS a part of the email encryption policies, TLS can be added as a delivery method by simply checking a box. By replacing the need for individual TLS configurations, ZixGateway allows your organization to skip the cost and time typically associated with each connection.
- Increased delivery control - No longer is TLS an all-or-nothing method. By making TLS a part of the ZixGateway policies, TLS is used only where appropriate.
- Reporting capabilities - ZixGateway offers superior visibility for compliance officers by providing reports that log how each message was delivered, including TLS encrypted email, and who it was delivered to.

- Branding of recipient messages - Embedded at the bottom of each TLS message is a "Secured by ZixCorp" note, providing confidence to your recipients that the email and its sensitive content were delivered securely.

Secure, bidirectional transparency, increased control, increased visibility and unique branding are features not available in competing TLS solutions.

Flexible Delivery

For recipients who do not have email encryption capabilities, ZixGateway offers two different delivery methods - ZixPort and ZixDirect. All of these options combine to create the ZixCorp Best Method of Delivery, which automatically determines the most secure and transparent method of sending your message.



ZixGateway Key Benefits:

- Offered an your location as an appliance or as a hosted service
- Quick deployment in less than a day
- Ability to send secure email to anyone
- No training for end users
- Implemented as an appliance or as virtual environment application
- Built-in content scanning
- Seamless integration with existing infrastructure and systems

ZixGateway Key Features:

- Full content scanning of message and attachments
- Centralized policy management
- Automatic retrieval and distribution of public encryption keys through *ZixDirectory*

- Corporate-defined policy management
- Flexible reporting capabilities
- Custom branding
- Message and attachment compression
- Interoperability with S/MIME and OpenPGP
- Support of TLS protocols
- Secure receive and reply for all recipients

ZixMail®

ZixMail is a desktop email encryption solution that provides individuals with a high level of security. It is an easy-to-use service that enables users to encrypt and decrypt emails and their attachments to anyone, with a single click. *ZixMail* can be downloaded and installed in minutes and integrates with all corporate email systems. The service provides automatic retrieval and distribution of public encryption keys through *ZixDirectory*. For extra convenience, certified receipts help senders know exactly when messages were sent and opened. *ZixMail* utilizes ZixCorp's *Best Method of Delivery*, if the recipient is not an existing ZixCorp customer, *ZixMail* will automatically send the message to a *ZixPort* ® secure portal, ensuring emails can be securely sent to any user, anywhere.

ZixMail Key Benefits:

- Easy to use
- Fast and easy to deploy
- Ability to send to anyone
- End-to-end delivery assurance
- No hardware to install
- Automatic public key exchange through ZixDirectory
- Compliant with existing systems

ZixMail Key Features:

- User-controlled operation
- Date- and time-stamped certified receipts
- Secure message storage
- Message and attachment compression
- Fully integrated version for Microsoft® Outlook®
- Requires minimal IT support
- Creation of certified receipts and non-refutable time stamps

ZixPort®

ZixPort is a secure messaging service that provides companies with a way to encrypt email communications with their customers and business partners. As a hosted service, branded for each customer, *ZixPort* does not require additional information technology (IT), web or security infrastructure. *ZixPort* is based on standard internet technology ensuring users can access their secure messages through a variety of browsers including browsers on mobile devices. With *ZixPort*, customers can customize the look and feel to match their web site and select from a variety of features to meet their needs. As a hosted solution, *ZixPort* requires little internal resource support, development time or hardware and it is easy for employees, customers and business partners to use. *ZixPort* is hosted in the *ZixData Center*SM for optimal security and availability. It also takes advantage of ZixCorp's unique

Best Method of Delivery and provides send-to-anyone capabilities for both *ZixGateway* and *ZixMail*.

ZixPort Key Benefits:

- Branding customization based on your organization's needs
- No software or user training needed
- Secure message send capability to anyone, anywhere
- No impact on internal IT resources or infrastructure
- Feature customization for optimum flexibility

ZixPort Key Features:

- User-controlled operation
- Unique support for portable and Smartphone devices
- Encrypted read and reply capabilities for all message recipients
- Secured compose capability for two-way communication
- Custom password policies tailored to your organization's needs
- Innovative message and attachment compression
- Address book with support for group distribution
- Automatic generation of notifications and invitations

ZixMobility ™

U.S. mobile users spend more time using e-mail on their phones than any other internet-based mobile activity. Yet, expectations of mobile users far surpassed existing technology in email encryption. Based on conventional, outdated email encryption standards, mobile email encryption users have struggled through rudimentary support, inconvenient steps, distorted layouts and cumbersome architectures. As a result, the power and benefits of secure email were severely stifled. ZixMobility addresses these challenges and elevates the standards for convenient secure email anytime, anywhere and on any mobile device.

A feature of ZixPort, ZixMobility enables business to stretch beyond conventional mobile limits by offering:

- Seamless email encryption as users navigate from desktop to mobile device
- Optimized layouts designed based on the user's environment
- Fully functional navigation maximized for the user's screen
- Maximum user convenience with no cumbersome steps

To ensure convenient delivery of secure email to your most valuable customers and business partners, ZixMobility is a standard ZixCorp feature, without any extra cost to ZixCorp customers.

ZixMobility Key Features:

- Seamless navigation between desktop and mobile device
- Screen layouts designed based on user device
- Maximized navigation based on user environment
- Extended email life of one year or more
- Functions across all internet-enabled mobile devices

ZixMobility Benefits:

- Convenient, secure email to your recipients through ZixPort at no extra cost
- Access to secure email without cumbersome steps
- No need to magnify and correct distorted layouts
- Improved productivity with real-time access to secure email

*ZixDirect*SM

ZixDirect is a delivery method that makes it possible to push an encrypted email directly to a user's inbox. With *ZixDirect* there is no client software to install or maintain, and the user does not need to have any decryption capabilities to read the message. Users receive secure emails directly in their inbox and have the ability to read secure messages while working offline. An extension of our corporate wide *ZixGateway* service, *ZixDirect* makes it easier to choose the method of delivery that best meets the needs of the user.

ZixDirect Key Benefits:

- Secure messages sent directly to recipient's email inbox
- Offline access to messages
- No additional software or training required
- Send-to-anyone capability
- Works seamlessly with existing systems
- Easy to deploy in under a day

ZixDirect Key Features:

- Ability to recover messages if password is forgotten No pre-registration required
- Automatic retrieval and distribution of encryption keys
- Custom branding
- Secure read, reply and forward capability

*ZixConnect*SM

ZixConnect is a managed TLS service that allows companies to secure their email communication to multiple partners using a single TLS framework. *ZixConnect* is for organizations that need to secure email communications with key business partners, but are concerned about the long-term complexity of managing multiple separate TLS connections.

A single customer TLS connection to the *ZixData Center* can be all that is needed to secure emails communications to all partners. ZixCorp handles the set up and maintenance of each

secure connection. *ZixConnect* is easy to set up and use. It deploys in just a few hours and is completely transparent to end-users.

Users send and receive messages that are encrypted in transit - no passwords, no hardware, and no software required. And, because the emails are in plain text within the corporate network, retention policies are maintained.

ZixConnect can also be used by existing *ZixGateway* customers that need to use TLS with certain business partners, but would rather not set up and maintain the TLS connection directly. ZixCorp works with the partners to set up TLS connections to the *ZixData Center* and then customers can send and receive emails through their *ZixGateway* appliance while their partners can send and receive using TLS.

ZixConnect Key Benefits:

- Secure email communications with key business partners
- No capital investment
- Deploys in just hours
- Transparent to end users
- No new customer hardware or software required

ZixConnect Key Features:

- Gateway design ensures email archiving compatibility
- Messages delivered to user in plain text
- Mandatory TLS ensures end-to-end security available

ZixDirectory[SM]

ZixDirectory is one of the largest email encryption directories in the world. It enables seamless and secure communication among its millions of members by providing a centralized directory for automated key exchange. As an added service provided with *ZixGateway* and *ZixMail*, the directory enables users to transparently send and receive encrypted emails without having to exchange certificates. In addition, when used with either *ZixGateway* or *ZixMail*, the directory makes it possible to send secure emails to anyone, anywhere, without pre-registration or configuration. By providing customers with an automated key management service, ZixCorp is able to greatly reduce the typical cost and complexity associated with email encryption solutions.

ZixDirectory Key Benefits:

- Access to email encryption directory
- Members include the federal banking regulators, state banking regulators and several departments of the U.S. Treasury
- Centralized and automated key exchange

ZixDirectory Key Features

- Capacity, scalability, and infrastructure to support encryption keys for every email address in the world
- Public key validation and distribution in real time
- Transparent email encryption between ZixCorp users

- No key repository or PKI infrastructure to install or maintain
- Enterprise email encryption deployment in less than a day
- Reduced cost and improved ease-of-use for the organization
- High availability guaranteed through SLAs

ZixEnable℠

Leading healthcare, financial, government and insurance organizations have turned to ZixCorp to help them meet regulatory requirements and to protect customer privacy in their email communications. Now those organizations are leveraging email encryption as a strategic communication platform through ZixEnable.

ZixEnable is application-generated email encryption that enables businesses to secure the delivery of large-scale email communication containing personal private information. ZixEnable can be used to distribute personalized marketing campaigns, financial and health statements or other sensitive communication that businesses want sent in a timely and secure manner.

By using ZixEnable, businesses can experience:

- Improved customer loyalty by enabling highly personalized email communications while protecting sensitive customer information
- Increased cost savings and efficiencies by delivering sensitive information via email rather than paper mail
- Reduced risk of violating privacy regulations like HIPAA when delivering customer statements in email communications

To gauge the impact of ZixEnable, customers receive detailed summary reports on your application-generated email communication. Reports can be generated daily or weekly and include information such as what email was sent, who they were sent to and whether the email was read and when. In addition, a monthly summary report provides an overview of the effectiveness of your customer communication.

Customer Snapshot

Large health plan (LHP) delivers explanation of benefits (EoB) securely with ZixEnable.

- LHP member opts in
- LHP sets application to generate EoB emails
- Each EoB email is encrypted and placed in LHP's branded portal
- A notification email is sent to the covered member's email address
- The member opens the notification and clicks the "Open Message" button to view the EoB

OVERVIEW OF THE SYSTEM AND APPLICATIONS

Components of ZixCorp's ZixData Center[SM], Email Encryption Services, ZixONE, and Hosted Services

The System is comprised of the following components:

- **Infrastructure**: The physical and hardware components of a system (facilities, equipment, and networks);
- **Software**: The programs and operating software of a system (systems, applications, and utilities);
- **Data**: The information used and supported by a system (transaction streams, files, databases, and tables);
- **People**: The personnel involved in the operation and use of a system (developers, operators, users, and managers); and
- **Procedures**: The automated and manual procedures involved in the operation of a system.

The components above are described through the key processes, personnel and control activities relevant to Security, Availability, Processing Integrity, and Confidentiality of ZixData Center[SM], Email Encryption Services, ZixONE, and Hosted Services, and complementary user entity controls.

ZixCorp's ZixData Center[SM], Email Encryption Services, ZixONE, and Hosted Services are described in the context of the normal course of operations, and may not address every user's scenarios. ZixCorp's control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the control activities are included in Section 4, they are, nevertheless, an integral part of ZixCorp's system description. The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

The information in the following sections describes the processes and controls for ZixCorp's ZixData Center[SM], Email Encryption Services, ZixONE, and Hosted Services necessary to fulfill the Trust Services Principles of Security, Availability, Processing Integrity, and Confidentiality.

BOUNDARIES OF THE SYSTEM

The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures and data necessary to provide its services. The boundaries of ZixCorp's system include applications and infrastructure that directly support the services provided to ZixCorp's clients. Any applications, databases, and infrastructure that indirectly support the services provided to ZixCorp's clients are not included within the boundaries of ZixCorp's system.

Principles and Related Criteria

This report is focused on the Security, Availability, Processing Integrity, and Confidentiality principles and does not include the Privacy Principle. The control activities related to risk assessment, monitoring and communication are further described in the following sections as they relate to the Trust Services Principles. The P*rinciples* are defined as follows:

- ***Security:*** *The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.*
- ***Availability:*** *The system is available for operation and use to meet the entity's commitments and system requirements.*
- ***Processing Integrity:*** *System processing is complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements.*
- ***Confidentiality:*** *Information designated as confidential is protected to meet the entity's commitments and system requirements*

A. SECURITY

ZixCorp has formal policies and procedures in place for daily operations including escalation and tracking procedures designed to address non-compliance. A dedicated compliance program is in place to help facilitate any violations or suspected violations.

Commitment to Competence

Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Specific control activities that ZixCorp has implemented to ensure that competent employees are deployed throughout the company include the following:

- HR management considers the competence levels for particular jobs and translates required skills and knowledge levels into written position requirements.
- Management assesses each job candidate to determine whether the candidate possesses the perquisite level of competence to hold the position.

- Background checks are performed by a third party investigative agency in accordance with provisions of the Fair Credit Reporting Act for all prospective employees.
- New employees are required to complete security and confidentiality training upon hiring in addition to undergoing background checks that are conducted by a third party.
- Existing employees are required to complete security and awareness training on an annual basis.
- Training courses are provided to new and existing employees in order to maintain and advance the skill level of personnel.
- Training materials are subject to review and approval on a quarterly basis and when changes to confidentiality related procedures occur.
- Performance evaluations are completed annually and results are retained in the employee's personnel file.
- Terminated employees access is communicated and removed timely by the data center manager.

ZixCorp has formal policies and procedures in place for daily operations including compliance procedures designed to address non-compliance. A dedicated compliance program is in place to help facilitate any violations or suspected violations.

Application Controls
Customer SLAs contain confidentiality statements regarding the use of information, limitations of use and agreements with third parties. Privacy statements documenting description of services, information sharing and disclosure, security, user requirements and information collection and use practices are documented on the corporate web site and any changes to confidentiality are identified in the privacy statement.

Media disposal procedures are in place to address the secure disposal of hardcopy and electronic media. A third party media disposal company is contracted for the destruction of hardcopy and electronic media. Individuals assigned to sanitize or destroy media must have security clearance level that is as high as the sensitivity of the information stored on the media.

Application Control
Web customers are required to review and agree to the terms and conditions when completing online payments for ZixMail. ZixGateway is configured with predefined lexicons for content scanning. ZixPort, ZixMail and ZixGateway service description manuals provide information guides to provide an overview of the system, security requirements and functionality.

Board of Directors and Audit Committee Participation
ZixCorp's control consciousness is influenced significantly by ZixCorp's board of directors and audit committee. Attributes include the board of directors' and audit committee's

independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interaction with internal and external auditors. Specific control activities that ZixCorp has implemented in this area include the following:

- A board of directors oversees management activities and meets on a quarterly basis to discuss matters pertinent to the organization's operations and to review financial results.
- An internal audit team is in place to guide the activities of the internal audit department and review the results of self-assessments.
- The internal audit team performs a documented audit task review on an annual basis.
- A Steering Committee monitors operations to help ensure activities are in accordance with IT governance, risk and compliance requirements.
- The Steering Committee reviews and approves corporate policies and procedures and on a quarterly basis. The latest policies and procedures are available on the ZixCorp intranet.
- The IT security administrator performs a system security and availability review on a quarterly basis.

Physical Security

ZixCorp has limited access for identified systems to individuals with job responsibilities requiring access. Access to data center infrastructure is restricted to badge access cards assigned to specific personnel. Visitors are required to register themselves at the front desk. In addition, visitors are required to be escorted by an authorized ZixCorp employee when accessing the facility. A badge access system controls access to and throughout the facility. Access to the data center is controlled via a RFID badge access reading coupled with biometric device authentication. Surveillance cameras are also used to monitor and record facility activity. Data center entrances are monitored 24 hours per day by operations personnel.

Information Security

The Network Operations Center is the hub of the Email Encryption and related *ZixData Center* services, monitoring hardware status in the main data center and off-site backup location. Personnel supporting the Email Encryption and related *ZixData Center* services are assigned specific roles and responsibilities, which are geared to annual performance evaluations. Service delivery and support personnel are divided into those holding "Trust-Plus" roles, which require data center access, and "Trust" roles, which do not require data center access. Data center, operations, security and network management personnel hold "Trust-Plus" roles and are provided with the data center access necessary to perform their duties.

ZixCorp email encryption services do not identify, record, process, summarize, or report any financial transactions of our user organizations. Additionally, ZixCorp does not maintain accountability for any client assets, liabilities, or equity.

Policies and procedures are defined for information security and system availability. The confidentiality and related security obligations are documented to include the classification, labeling, and handling of data. Classifications are in place to identify and define the data and systems requiring restricted access. Physical and logical access is assigned through use of a standardized form that is approved by appropriate ZixCorp security individuals.
Users with access to client systems and data are required to sign acknowledgement forms. The ability to logon to production systems is restricted to individuals with job specific responsibilities. Predefined trust roles are defined and privileges are assigned based on required access levels. Users must authenticate themselves via user account, passphrase, and RSA token. The ability to logon to the production environment is restricted to the use of Secure Shell. Administrator access is further restricted to a select group of personnel.

Application users are required to verify email addresses for use with email encryption products and services. In addition, users are issued unique keys for message encryption and transmission. Authentication occurs via a user account, password and unique key before access is granted. Passwords are encrypted utilizing an MD5 one-way hash for ZixPort customers including ZixPort London customer.

Data Communications
A firewall system is in place and configured to filter unauthorized traffic. Intrusion detection is utilized to analyze events and send e-mail notification. In case of a breach, a commercial monitoring system is in place to provide notification. Internal network vulnerability assessments are performed on a weekly basis. External scans of the production network are performed on a quarterly basis. Incidents are documented and reviewed by network operation specialists on a weekly basis. Virtual private network is utilized to secure the remote access to the production environment. To secure customer confidential emails, a minimum of 128-bit encryption is used.

Secure emails are delivered to non-ZixCorp clients through ZixPort and ZixPort London. All ZixCorp services utilize real-time clocks that are synchronized to a common Network Time Protocol service.

B. AVAILABILTY

ZixCorp's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored.

Environmental Integrity

The data center is equipped with air conditioning units in a redundant configuration. The units are inspected on a quarterly basis by a third party. Two Uninterruptible Power Supply (UPS) systems are connected to the units providing temporary electricity in the event of a power outage. The UPS systems are also inspected on a semi-annual basis by a third party. The data center is supplied with electrical power from two independent power grids. In addition, the data center is equipped with a diesel generator to provide additional power in the event of an outage. Fire detection and suppression controls such as smoke detection devices and a FM200 system protect the data center. The fire suppression and alarm systems are inspected on a semi-annual basis by a third party.

Computer Operations

Availability policies and procedures are defined and documented to guide personnel in identifying and mitigating risks in the production environment. Multiple and redundant internet service providers and load balancing are built into the system infrastructure. The mirroring of customer keys and account data to alternate hot site locations is performed. For Email Encryption, a warm site is maintained with a collocation center that is geographically separate. Production configurations are backed up on a weekly basis to the alternative back-up site. A documented audit and restoration of applicable backup data is performed quarterly.

Incident Management and Monitoring

Documented incident management policies and procedures exist and define responsibilities, severity levels and escalation procedures. A commercial ticketing system exists to manage incidents, response and resolution. A root cause analysis (RCA) is performed for customer impacting incidents. Network operations personnel monitor system event log, identify new events, and respond to identified events. Personnel also provide customers with 24 hours per day local and remote monitoring of ZixGateway hardware. Personnel also monitor availability statistics 24 hours per day for comparison with availability commitments.

Business Continuity

ZixCorp has implemented policies and procedures for business continuity and disaster recovery. The Compliance Officer reviews the Business Continuity Plan and Disaster Recovery Plan on an annual basis. The Risk Management Steering Committee conducts system availability and system security reviews and makes recommendations to management on a quarterly basis. In addition, the disaster recovery systems are tested on an annual basis.

C. PROCESS INTEGRITY

The Risk Management Steering Committee holds a quarterly meeting to discuss and review operational activities regarding internal/external audit recommendations, access reports and system capacity.

Systems Maintenance
Standard server builds are in place for the creation and installation of production hardware and software. These procedures are run by scripts.

Patch management procedures are in place for initiation to deployment through use of a dedicated patch management system. Patch management is managed by the Systems Engineer and the patch application is configured to restrict automatic installation of patches.

Change Management
Formal documentation of changes to system configurations, software, hardware, network components and maintenance activities is required. Emergency response and resolution procedures have been developed and supported by appropriate automated tools. Automated procedures are used wherever possible for routine procedures such as backups. Specialized tools are used for managing change requests, customer contact, user support and problem tracking.

Management determines the required level of segregation of duties to ensure development, quality assurance, and deployment personnel are appropriately organized. Software development management and developers hold “Trusted” roles and are not provided with data center access.

A change request form documents software change requests, authorization, testing, and approval. Change requests are categorized by priority level and authorized by the IT Steering Committee prior to deployment. A commercial tracking system is used to document change requests, workflow, testing, and approvals. Any changes to the production infrastructure are tested and approved prior to implementing. Changes follow a change management process that requires changes not only to be tested before promotion to production, but developed and tested in separate environments. No changes that would affect user systems are performed and therefore communication to the user of changes to ZixCorp systems occurs. The development and test (QA) environments are physically separated from the production environment within the data center. Emergency changes are implemented solely by the Trust-Plus administrators. The Integration Manager reviews and approves emergency changes. The IT Steering Committee approves the introduction of new infrastructure or changes to existing infrastructure. Development, quality assurance and integration teams meet daily to discuss potential production issues.

D. CONFIDENTIALITY

ZixCorp has formal policies and procedures in place for daily operations including compliance procedures designed to address non-compliance. A dedicated compliance program is in place to help facilitate any violations or suspected violations.

Application Controls
Customer SLAs contain confidentiality statements regarding the use of information, limitations of use and agreements with third parties. Privacy statements documenting description of services, information sharing and disclosure, security, user requirements and information collection and use practices are documented on the corporate web site and any changes to confidentiality are identified in the privacy statement.

Media disposal procedures are in place to address the secure disposal of hardcopy and electronic media. A third party media disposal company is contracted for the destruction of hardcopy and electronic media. Individuals assigned to sanitize or destroy media must have security clearance level that is as high as the sensitivity of the information stored on the media.

Application Control
Web customers are required to review and agree to the terms and conditions when completing online payments for ZixMail. ZixGateway is configured with predefined lexicons for content scanning. ZixPort, ZixMail and ZixGateway service description manuals provide information guides to provide an overview of the system, security requirements and functionality.

Control Environment
ZixCorp's control environment reflects the overall attitude, awareness, and actions of ZixCorp's management, and other stakeholders concerning the importance of control and its emphasis within the entity. The organizational structure, separation of job responsibilities by departments and business function, documentation of policies and procedures and internal audits are the methods used to define, implement and assure effective operational controls. Relevant aspects of the ZixCorp control environment that affect information technology processes and systems are summarized in this section of the report, *Security*.

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 the control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of ZixCorp's ethical and behavioral standards, how they are communicated, and how they are reinforced in

practice. 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 ZixCorp values and behavioral standards to personnel through policy statements and codes of conduct and by example. Specific control activities that ZixCorp has implemented in this area include the following:

- Documented organizational and employee policies are in place that communicate entity values and behavioral standards to personnel.
- Management reviews and approves documented policies and procedures on an annual basis.
- A background check is performed for employees as a component of the hiring process.
- Employees are required to complete a new hire orientation that includes training in the company's policies and procedures contained within the code of ethics.
- Employees are required to sign the employee handbook on an annual basis to confirm their understanding of and compliance with the policy.
- Employees are required to sign a confidentiality agreement as a component of the hiring process agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.

Management's Control Philosophy

ZixCorp management is committed to maintaining the highest levels of ethics and integrity. Management endeavors to foster this culture by promoting cooperation, coordination, communication, and alignment of interests within and among ZixCorp employees, customers and other involved parties. As a matter of policy, all ZixCorp employees are required to review the ZixCorp Employee Handbook annually. New employees and existing employees are also required to complete security and confidentiality training upon hiring for new employee's and annually for existing employees. Any updates to training materials in regards to confidentiality related procedures are appropriately reviewed and approved quarterly. A copy of the employee's acknowledgement is kept in their employee file. The Risk Management Steering Committee reviews and approves corporate policies and procedures, found on the ZixCorp Intranet, on a quarterly basis. The same committee oversees management's activities, ensuring policy compliance and completion of a quarterly risk-based assessment. Each department also meets regularly to discuss current matters. The CISO is responsible for development and maintenance of security policies and creating a control-conscious environment.

Risk Assessment

ZixCorp operates in a dynamic market, utilizes complex technologies and processes, and is experiencing growth. ZixCorp's clients operate in a highly regulated, control-conscious environment. Therefore, it is vitally important for ZixCorp to be able to identify the potential impact of changes to the operating effectiveness of existing controls and the need for modified or new controls. ZixCorp's risk assessment process generally consists of the following elements:

- Assessing the sufficiency of corporate policies, procedures, systems and other arrangements in place to control risk.
- Identifying potential risks in ZixCorp's technology, products, security and services.
- Determining the level of severity for identified risk factors when evaluating the potential impact of the identified risk factors on the operating effectiveness of existing controls.
- Identifying potential sources of risk and recommending areas for management to develop and implement policies and procedures to mitigate the identified risk areas.
- Monitoring and evaluating the operating effectiveness of existing controls in light of changes resulting from growth, new or renovated information systems, regulatory changes, new personnel and external security risk factors.
- Monitoring the regulatory environment to determine the effect that proposed and new regulations may have on ZixCorp's service offerings.

Monitoring

ZixCorp's management and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, ZixCorp has implemented a series of "key indicator" management reports that measure the results of various processes involved in processing transactions for user organizations. Key performance indicator reports include actual transaction processing volumes compared with historical trends, actual processing load compared to historical trends, and actual system availability and response times compared with established service level goals and standards. All exceptions to normal or scheduled processing related to hardware, software or procedural problems are logged, reported and resolved daily. Key performance indicator reports are reviewed weekly by appropriate levels of management and action is taken as necessary as described in detail within this section**.**

Information and Communication

Various direct and indirect methods of communication are implemented by management to ensure employees understand the policies, procedures, standards, and guidelines developed to define their individual roles and responsibilities. Examples of these methods include orientation and training for new employees, emails, ongoing training, distribution of policies and procedures and on-the-job training.

Monitoring of the Subservice Organization

Zix utilizes Via West and Equinix for co-location services in Austin, TX and Slough, U.K. Management of Zix receives and reviews the SOC reports of Via West and Equinix on an annual basis, including the complementary subservice organization controls (CSOC) included within the Via West and Equinix reports. In addition, through its daily operational activities, management of Zix monitors the services performed by Via West and Equinix to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also holds periodic calls with the subservice organization to monitor compliance with the service level agreement, stay abreast of changes at the subservice organization, and relay any issues or concerns to the subservice organization management.

DESCRIPTION OF COMPLEMENTARY USER ENTITY CONTROLS

ZixCorp services was designed with the assumption that certain controls, policies and procedures would be implemented by user organizations to ensure that all activities related to the ZixCorp services are appropriately authorized and secured. Complementary user entity control considerations are expected controls of the user organization however, expected controls are not critical for ZixCorp to achieve the Trust Services Principles. User organizations should have the following expected controls to complement the ZixCorp controls in place that independently meet the required the Trust Services Principles and Criteria in Section IV of this report.

- Changes to processing options (parameters) are required to be noticed, appropriately authorized, approved and implemented.
- User access to ZixPort is appropriately administrated by user organizations:
  - Passwords are changed periodically
  - Passwords are kept confidential
  - Security violations are monitored and followed up on as necessary
- ZixPort User organizations are responsible for authorizing a data retention period greater than the Zix standard of 14 days.
- ZixPort user organizations are responsible for installation and updates to antivirus software on critical servers and desktops.

The list of user-organization control considerations presented above and those presented with certain specified Trust Services Principles do not represent a comprehensive set of all the controls that should be employed by the user organization. Other controls may be required.