

Attachment C

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and MARCUK TECHNOLOGY (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited, to personally identifiable: student data, student demographics, scheduling, attendance, grades, health and discipline tracking. Protected Data also includes all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts that ESBOCES and/or the participating school district has identified to Contractor in writing as sensitive or confidential data of ESBOCES and/or the participating school district. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,

-AND-

Personally identifiable information from the records of ESBOCES and/or participating school districts relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy provided to Contractor in advance of executing this Agreement. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall delete all of ESBOCES' and/or participating school districts' Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;
6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option, or direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:


1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;
3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:
 - a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or
 - b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, ESBOCES or the institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;
7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

<CONTRACTOR>
BY: 

DATED: 6/30/2022

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

<https://zix.com/privacy-policy>

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

**EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY**

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians, and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. Eastern Suffolk BOCES wishes to inform the school community of the following rights:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record maintained by Eastern Suffolk BOCES.
3. State and Federal laws protect the confidentiality of personally identifiable information and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or, by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, NY 12234
CPO@mail.nysed.gov.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into contracts with certain third-party contractors. Pursuant to such contracts, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract

Eastern Suffolk BOCES enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

Answer: Marcum Technology has no access to any data

From the Zix Privacy Policy, under the " How we use the information that we collect" Section

Zix uses information about you for our legitimate interests and business purposes, including as follows:

- To provide you with products, services and any renewals thereof, including but not limited to anti-spam, anti-virus, email archiving, email encryption, email hosting, and transmission services;
- To process your registration including verifying the information you provide is active and valid; In our Zix Services, to facilitate secure messaging with third parties;
- To communicate with you including via email or push notification; To monitor compliance with our Terms;
- To notify you when you receive a Zix service email message, when a Zix service email message has failed or expired, when an intended recipient has picked up an email message you sent (if you so request), when multiple attempts to enter your Zix service passwords have failed on our Site, and when there is any change in our Terms or in the availability of various products and services;
- To communicate with you concerning problems or malfunctions that you report; To provide you with support and maintenance for products and services;
- To notify you of any changes to your use of our Site, products, or services; To respond to your inquiries;
- To bill you for product and services;
- To investigate, prevent, or take action regarding illegal activities, suspected fraud, safety of person or property, or violation of our policies or our other rights or interests;
- To monitor traffic patterns and Site usage and where applicable report on traffic levels and/or statistics to certain enterprise customers, such as how many of their users are sending emails and from what departments.
- To test, analyze and improve our services and marketing; To market existing and new Zix services.

2. How the third-party contractor will ensure that the subcontractors, persons, or entities with whom the third-party contractor will share the student data or teacher or principal data, if any, will abide by data protection and security requirements;

Answer: Marcum and Zix will abide by both GDPR and CCPA

3. When the contract expires and what happens to the student data or teacher or principal data upon expiration of the contract;

Answer: From the Zix Privacy Policy, under the "Data Storage" Section:

Zix stores only the salted hash of a Zix service password. This means that we don't hold your Zix service password itself but rather a unique encrypted version of it. ZixMessage Center email messages that you send or receive via Zix services will ordinarily expire from our disk storage

systems based on the expiration time set by the sender at the time the email was sent (1 to 365 days from the day the email message was sent). If you request deletion of your Zix service account, that account will be deactivated and your email address and information will be removed from our user registration database associated with that Zix service within 30 days, subject to any need we have to hold onto the data for longer to meet any legal, auditing or regulatory requirements and subject to any commitments we have given to third parties – for example your employer if your employer paid for your Zix Company Service account. You can also request deletion of all your Zix Company Service accounts. If we do delete any of your accounts, those accounts will be reinitiated if another email is sent to you using a Zix Company Service. Email header information maintained for purposes of transaction logging, and user account information maintained for disaster recovery purposes, will be held longer than the content of email messages, as described above, in order to provide Zix Company Services, and support, including technical support and business continuity, to our customers."

4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data collected; and

Answer: Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway, Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:
Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234
CPO@mail.nysed.gov.

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security) and the security protections taken to ensure that such data will be protected, including whether such data will be encrypted.

Answer: From the Zix Privacy policy under the "Data Storage" section:

"Most account information (including email addresses, public keys, names, and mailing addresses, but excluding credit card information used for payment to Zix) is stored on multiple disk storage systems at our data centers in the United States or Canada, This means that we redundantly store data on more than one server in one of those locations.

Furthermore, from the "Security" Section:

"Zix takes reasonable precautions, including the maintenance of reasonable physical, electronic, and procedural safeguards, to help protect your information from loss, misuse, and unauthorized or illegal access, disclosure, alteration, modification, use or destruction. Zix has implemented reasonable security measures to help protect your email address and the Zix service passwords associated with your email address from unauthorized access or disclosure, alteration, unlawful

destruction or accidental loss. When appropriate, Zix uses industry-standard encryption to protect certain data (e.g., credit card numbers) during transmission. The servers on which we store your information are kept in an environment that is controlled and monitored 24 hours per day, 7 days per week."

Third-Party Contractors are required to:

1. Provide training on Federal and State law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to educational records to those individuals who have a legitimate educational interest in such records;
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
5. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all State, federal, and local data security and privacy contract requirements will be implemented over the life of the contract; and
9. Provide a signed copy of this Parents' Bill of Rights to Eastern Suffolk BOCES, thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Parents' Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this signed document must be made a part of Contractor's Data Security and Privacy Plan.



Privacy Policy

(Last Update and Effective Date June 6, 2022)

Purpose of this Policy

Zix Corporation and its subsidiaries ZixCorp Systems, Inc. and ZixCorp Global Inc., 2711 N. Haskell Ave. Suite 2200, Dallas, TX 75204-2960, Greenview Data, Inc. ("Greenview Data"), 8178 Jackson Road, Suite A, Ann Arbor, MI 48103, and CM2.COM, Inc. dba Erado ("Erado"), 321 Burnett Ave. South #100, Renton, WA 98057, Total Defense LLC ("Total Defense"), 1393 Veteran Memorial Highway, Suite 310N, Hauppauge, NY, App River, LLC ("AppRiver"), 1101 Gulf Breeze Pkwy, Suite 200, Gulf Breeze, FL 32561, and Roaring Penguin Software Inc., now AppRiver Canada ULC ("AppRiver Canada"), 300 March Road, Suite 304, Ottawa, Ontario K2k 2E2 Canada (collectively, "Zix," "we," "us" or "our"; each "a Zix Company") operate Web sites located at zix.com (with the exception of investor.zixcorp.com), secure-zixcorp.com, zixmessagecenter.com, zixmessagecentre.com, zixit.com, powerofeveryone.com, spamstopshere.com, greenviewdata.com, erado.com, appriver.com, roaringpenguin.com, and totaldefense.com, their subdomains (collectively, the "Sites"), through which users can obtain information about Zix and subscribe to various security services provided by Zix (collectively, the "Zix Services" or the "Zix Company Services"), and mobile applications including ZixOne, Total Defense Mobile Security, and the DeliverySlip Apps (the "Apps"). AppRiver Canada conducts business under the name Delivery Slip. AppRiver has subsidiaries AppRiver UK Ltd., Venture House, 2 Arlington Square, Brackness, Berkshire RG121WA, UK and AppRiver AG Industriestrasse 33, 5242 Lupfig, Switzerland. The investor.zix.com website is operated as described here.

Contents

- Scope of this Policy
- Potential applicability of other privacy policies
- Applicability of other terms
- Information that we collect
- Information that we automatically collect
- IP addresses and location information
- Logs
- Cookies
- Web Beacons
- Embedded Scripts
- Information that third parties provide about you
- How we use information that we collect
- Emails and attachments
- Employment applications
- Information sharing and disclosure
- Analytics and advertising
- Social Features
- Google API Services
- Links and online tracking by third parties
- Your ability to manage your Zix Company account information
- Security
- Data storage
- Guidelines regarding children
- Your California privacy rights
 - Shine the Light Customer Rights
 - California Consumer Rights Under the CCPA
- European privacy rights
- Data Controller
- Lawful basis for processing
- Privacy Shield
- Notification of changes to this Policy
- Privacy Policy questions, suggestions and complaints

Scope of this Policy

This Policy applies to individuals that subscribe to and use any Zix Company Service, as well as individuals that do not subscribe to or use any Zix Service but have sent or received emails to or from users or subscribers of Zix Company Services or who visited the Sites or Apps. This Policy applies to all information collected through the Sites and Apps, regardless of how you access the Sites or Apps. That is to say, this Policy applies whether you are accessing our Sites on a computer or on a mobile device like a tablet, or phone. We may also speak with you face to face (for example at a conference) or by telephone (for example when you make a support call). Those conversations are also covered by this Policy. By providing information to us when subscribing, contacting or communicating with us, or using the Sites, Apps, or Services, you expressly agree to this Policy.

This Policy does not apply to information collected through any third party products or services, even if resold by Zix.

Potential Applicability of Other Privacy Policies

You might use Zix Company Services through a web portal provided by us on behalf of our customer, such as your employer, healthcare provider or financial institution. In that case, your employer, health care provider or financial institution likely also has its own privacy policy that applies to your use of the Zix Services, and both privacy policies apply to you in those situations. Zix is not responsible for the privacy practices of third parties. If you are a data subject located in Europe, please see the section below entitled "Data Controller" for more information on our relationship with our customers.

Applicability of Other Terms

Information collected by Zix through its password protected sites and through customer use of the Zix Company Services is also governed, to the extent applicable to the relevant Zix Company Services, by Zix's Terms and Conditions, Zix's License and Services Agreements for the applicable Services, Zix's End User License Agreements, the Greenview Data Services Agreement, Erado's Terms and Conditions, the SpamStopsHere Specific Terms, AppRiver's Terms of Subscription, and other applicable Services Agreements (collectively, "Terms"). Please carefully review those Terms.

Information That We Collect

Zix collects information that you voluntarily provide when: using the Sites, Apps, and our products or Services; participating in our surveys, contests, and other promotions; registering for Zix Services, Sites, Apps, events, or resources; subscribing to our email listings; applying for a job; or communicating with us or requesting that we contact you (including through customer support). The information we collect includes information relating to identified or identifiable natural persons. Examples of information we collect include: contact information, such as names, mailing addresses, email addresses, and phone numbers; financial information, such as credit card number numbers; credentials, such as passwords, password hints, and authentication data; content data, such as the content of the messages you send to us for customer support, feedback, and product reviews; purchase data, such as purchases you have made, items in your shopping cart, and how often you make purchases; demographic data, such as preferred language; and resume data, such as your employment history, transcript, writing samples, and references. We also collect broad demographic and statistical information, such as your state and county of residence.

Zix collects your contact information described above when you register to use the Zix Services. Zix also receives and records your name and the credit card information that you supply if you pay to use the Zix services. In addition, Zix collects a variety of information about users and subscribers to Zix Services and about other individuals that send or receive email to or from such users and subscribers, including contacts, IP address, and relationships. That information includes, without limitation, email address, Zix services passwords and passphrases, email message content, and information about Zix email accounts. We also collect metadata about emails, such as header information (e.g., sender, recipient, time sent, to, from, cc, date, subject line), file structure, operating systems used, system components, and hardware used. These types of metadata information are not encrypted by Zix because they are required for email delivery and analysis. The content of

email messages and attachments (including non-spam messages) will not always be encrypted if you use the advanced threat protection services, including but not limited to during spooling for delivery and on the way to quarantine. Further, you understand that we can perform a manual review of the email content to identify threats, which includes some non-spam messages and identified threat information is shared with Zix subsidiaries and may be shared with third-parties.

If you use the Erado services, we collect communications information for archival purposes on behalf of, and as directed by, our customers. This information includes emails, texts, websites, social media messages or posts, and other forms of data or electronic communications; it also includes data about our customers and the third parties with whom they correspond.

If you or your company uses ZixOne, we automatically collect the phone number of the device on which the application is accessed and compare it to the PIN you set to access the application. Depending on your company's arrangement with Zix, either Zix or your company (or their respective service providers) maintains the back-end servers that support ZixOne. Zix or your company has the ability to determine which message(s) you are viewing when you use ZixOne.

Our AppRiver SecureSurf® Service is designed to protect users from malware, allow employers to restrict employee access to inappropriate websites, and give employers the ability to track and collect the web histories of their employees. As a result, we obtain a limited amount of web surfing history.

If you choose to refer a friend or business entity to Zix, we will ask you for certain information about your friend or a contact at the business entity. We may contact the referred party using the contact information you provide (such as by email, postal mail, landline phone, and mobile phone, as applicable). Zix stores this information for its marketing purposes, to track the success of the referral program, and to determine our obligations under the referral program. Individuals referred through our consumer referral program may contact us at privacy@zixcorp.com to request that we cease contacting the individual in connection with the referral program.

When you request technical support, Zix collects your name, employer, email address, mailing address, and phone number in order to provide this requested service to you. You have the option of providing additional information to support including your demographic information (such as your state and country of residency), operating system, browser, Internet service provider ("ISP"), connection type and email program that you are using. We encourage you to provide the additional information so that we can determine specific regional problems (such as natural disasters or power outages caused by cuts through fiber

optic cable) or isolate problems relating specifically to your particular operating system, email program or browser, thus enabling us to provide a more accurate response to your support requests.

Information That We Automatically Collect

Zix automatically receives certain information about your device and how your device interacts with our Site. Examples of such information include your device's IP address and other device identifiers, device type, browser type (such as Chrome®, Firefox®, Internet Explorer® and Safari®), browser language, operating system, referring and exit page, pages visited, number of clicks, domain names, error reports, performance data, and time spent on our Site. We use various current – and later – developed tracking technologies to collect this information, including cookies, web beacons, and embedded scripts. Zix combines such information with other types of data it collects about you, such as your email address. Zix treats any such combined information as personal information under applicable laws and will treat any such information in accordance with this Policy.

IP Address and Location Information

When your Web browser or email application requests content from another device on the Internet, it automatically gives that device the address where the requested information should be sent. This is called your device's "IP address." (IP stands for "Internet Protocol.")

Zix and our service providers receive your IP address each time you obtain content from the Site. We use your IP address for various purposes, including diagnosing service or technology problems that are associated with your IP address, conducting analytics, and estimating the total number of users visiting the Site from specific locales, countries or regions of the world. An IP address generally indicates a user's physical location. Zix generally does not collect precise location data (such as GPS or mobile device coordinates); however, when you install certain Apps like Total Defense, you will be asked to grant access to your mobile device's geolocation data. If you grant such permission, Zix collects information about your precise geolocation information (i.e., your real-time geographic location), and uses that information to provide or customize the Apps with

location-based information and features. IP addresses and access times are linked to your email address, but this combined information is for our internal use only and is not shared with third parties.

Logs

When you request content from the Site, information related to that request is collected and stored in log files on our servers. That information includes the date and time of the request, and the IP address of the device that requested the content. We use log files for debugging, troubleshooting purposes and delivering messages using DeliverySlip messaging products. For example, when you send or receive a message using DeliverySlip, we need to collect the content of that message to deliver it to an inbox, display it to the recipient, enable the ability to reply to it, and store it until the recipient decides to delete it. For messaging functionality, we collect certain kinds of data, such as the content of communications sent or received including attachments such as files for e-signature or documents, photos, music, or videos and the subject line and body of a message. DeliverySlip encrypts attachments, e-signature documents and the body of messages at rest and transports the content of communications using HTTPS (TLS 1.1 or higher).

Cookies

If you visit the Zix Sites, or use certain Zix Services, Zix and our service providers will set cookies and similar technologies on your computer and/or your mobile device and later access those cookies in order to deliver services. A cookie is a small text file, which often includes a unique identifier, which is sent to your browser when you visit a Web site. It is then stored on your computer or mobile device. Zix uses cookies to allow you to use certain functions when you use various Zix Company Services, and to engage in interest-based digital advertising as described below in the Section entitled "Analytics and Advertising." Please read our **Cookie Notice** for further information about the types of cookies we set including information about how to control or delete cookies; note that our Cookie Notice

does not apply to the Greenview Data or Erado services or websites, including but not limited to SpamStopsHere.

If you do not accept cookies or disable these technologies, you will not be able to use all portions or functionality of our Sites and/or Services.

Web Beacons

Small graphic images or other web programming code called web beacons (also known as "clear GIFs"), which are invisible to you, are included in our web pages and e-mail messages. Web beacons are used for a number of purposes, including, without limitation, to count visitors to the Site, to monitor how users navigate the Site, to count how many e-mails that were sent were actually opened or to count how many particular links were actually viewed.

Embedded Scripts

An embedded script is programming code that is designed to collect information about your interactions with the Site, such as the links you click on. The code is temporarily downloaded onto your device from our server or a third party service provider, is active only while you are connected to the Site, and is deactivated or deleted thereafter.

Information That Third Parties Provide About You

We receive information about you from third parties who are lawfully permitted to share your information with us. For example, if you are on another web site and you provide information that the website operator indicates will be provided to Zix, that website operator will typically forward the information you provide. We may contact you using the information you provided, in accordance with your communication preferences. We also

combine the information we receive from third parties with information we collect or already maintain in order to ensure the records we hold about you are accurate and up to date, among other things. For example, if your company provides you with access credentials to the ZixOne App, we receive information about you from your company to provide you with access to the App and your related company Exchange account. We combine information we receive from your company with information we collect through ZixOne. In those cases, we will apply this Policy to the combined information, plus any additional restrictions imposed by the source of the data.

To enhance user experience, some DeliverySlip Client Applications provide integration capabilities with Google G Suite™ and Microsoft Office 365™. In such cases, Zix will have access to emails; calendar data; files and folders data, such as those stored in Google Drive or Microsoft OneDrive; and contact data.

In addition, we supplement the information we collect with outside records from third parties in order to provide you with information, services or goods you have requested, to enhance our ability to serve you, and to tailor our content to you. These third party sources vary over time, but have included data brokers from which we purchase demographic data, third party partners and resellers, our customers, social media platforms, lead generation providers, content sponsors, and publicly-available sources such as open government databases or data in the public domain. We combine the information we receive from those other sources with information we collect through the Sites, Apps, and/or Services. In those cases, we will apply this Policy to the combined information, plus any additional restrictions imposed by the source of the data.

How We Use Information That We Collect

Zix uses information about you for our legitimate interests and business purposes, including as follows:

- To provide you with products, services and any renewals thereof, including but not limited to anti-spam, anti-virus, email archiving, email encryption, email hosting, and transmission services;
- To process your registration including verifying the information you provide is active and valid; In our Zix Services, to facilitate secure messaging with third parties;

- To communicate with you including via email or push notification; To monitor compliance with our Terms;
- To notify you when you receive a Zix service email message, when a Zix service email message has failed or expired, when an intended recipient has picked up an email message you sent (if you so request), when multiple attempts to enter your Zix service passwords have failed on our Site, and when there is any change in our Terms or in the availability of various products and services;
- To communicate with you concerning problems or malfunctions that you report; To provide you with support and maintenance for products and services;
- To notify you of any changes to your use of our Site, products, or services; To respond to your inquiries;
- To bill you for product and services;
- To investigate, prevent, or take action regarding illegal activities, suspected fraud, safety of person or property, or violation of our policies or our other rights or interests;
- To monitor traffic patterns and Site usage and where applicable report on traffic levels and/or statistics to certain enterprise customers, such as how many of their users are sending emails and from what departments;
- To test, analyze and improve our services and marketing; To market existing and new Zix services;
- To resell, and sometimes provide support for, the offerings of third parties including Microsoft; To inform you of any new or updated services or product offerings; and
- To provide tailored content and advertising.

We also use information about you with your consent, including as follows:

- To market existing and new Zix services to the friends or businesses you refer to Zix;
- To manage your participation in our surveys, contests, events, and other promotions; and
- To fulfill any other purpose disclosed to you and with your consent.

Emails and Attachments

Zix uses email message and attachment content in order to provide and improve our products and services. For example, if you request that Zix host and operate a ZixGateway appliance on your behalf (the Zix™ Hosted Services), we automatically scan outbound email and attachments to determine whether they should be encrypted in accordance with your policies, and to provide you with usage reports and to improve our email filters; and

we collect and retain the content and attachments of outgoing email messages until they are delivered or the messages expire in accordance with your policies. Likewise, if you subscribe to our advanced threat protection service, we automatically and manually (with your consent) scan inbound email and attachments to protect you against advanced threats and to provide you with usage reports and to improve our email filters; and we collect and retain the content and attachments of inbound email messages until they are delivered or the messages expire in accordance with your settings.

We primarily use the information we collect when you use the ZixOne App to provide you with access to your Exchange account and in connection with your relationship or your company's relationship with Zix. To provide and enhance App performance, the back-end servers that support ZixOne (which may be hosted by Zix, your company, or their respective service providers) use and retain temporarily (which should usually not exceed a few days) emails, attachments, contacts, calendar items and other Exchange content (collectively "Exchange content") that you access and view. The Exchange content is temporarily cached on your mobile device until you exit the App. For example, the App accesses and downloads some of your contacts from your Exchange account when you use the App, such as to send an email.

Please be aware that the App, like all other apps, runs in the background on your mobile device until you take steps to exit the App. Please follow the directions from your mobile device manufacturer in order to exit the App. The back-end servers sometimes retain Exchange content even after you exit the App.

Employment Applications

If you use the Site to apply to work with us (for example via www.zix.com/company/careers) we will use the information you supply to process your application and to monitor recruitment statistics. We retain statistical information about applicants to help inform our recruitment activities. Zix is headquartered in the United States and employee and recruitment data is held there and in other Zix locations worldwide. Once a person has taken up employment with us, we will compile a file relating to their employment. At that stage we will give the employee more details about how we hold employee data.

Information Sharing and Disclosure

Subject to recent changes in the law, which may include a different definition of “sell” from those previously used in this policy (further discussed below), Zix generally does not sell or rent your information, except in the event that Zix (or some or all of its assets) is merged with, sold to, or otherwise transferred to, one or more third parties. In such an event, customer information might be included among the transferred assets and Zix reserves the right to disclose information it has about you for our business purposes including those described above in the Section entitled “How We Use Information That We Collect.” Notwithstanding any such transfer, your information will remain subject to this Policy. Our customer database could be sold separately from the rest of the business, in whole or in a number of parts. It could be that the purchaser’s business is different from ours too. If we are involved in a merger, acquisition, or sale of all or a portion of our assets, you will be notified via email and/or prominent notice on our Web site for 30 days of any change in ownership or uses of your information, as well as any choices you have regarding your information.

In addition, depending on the Zix Company Service(s) you use, Zix shares or discloses your information, and the information of your friends, family, or of others to whom you refer Zix, for business purposes as described below. The information so shared or disclosed includes the categories of information described above in the Section entitled “Information That We Collect”; public encryption codes for your email address; and information about your account usage (including the number of email messages and attachments, if any, that you sent; the list of recipients; and the subject and size of the combined text body of those email messages and attachments). We share:

- with persons or companies we retain to carry out or provide support to Zix (“Service Providers”) and our legitimate interests and business purposes described in the Section entitled “How We Use Information That We Collect”. We contractually require that those Service Providers use information they obtain from Zix solely for the purpose of providing these services, although we permit them to use aggregate information that does not identify you for other purposes.

Following is additional information about the vendors with whom we work across all our various product offerings. Zix and its affiliates may also provide these types of services in providing the Services to you.

Internet Infrastructure

We may use Cloud hosting and back-up, ISP, Local Loop, Distributed Denial of Service (DDoS) and other Internet infrastructure vendors to connect our network to the Internet and co-location managers to provide data center infrastructure and physical security.

Service-Management Operations

We may use various vendors for administrative and solution-management purposes, such as billing, analysis, alerting, customer management, and marketing communications.

Furthermore, we may use vendors for support services and the delivery of maintenance upgrades or other development of the Services (to include platform development tools).

- with your employer and/or compliance review committees for billing and auditing purposes. Your employer and/or the compliance review committee may be based in a different country from where you are based. This could mean that we would disclose your data to them anywhere in the world. By using our service you consent to that disclosure. Please note with regard to ZixOne, that your company or employer also has the right or ability to access information stored, sent, received, or accessed on or through your Exchange account, independent of your use of the App. Depending on your company's arrangement with Zix, your company or its service providers - rather than Zix - may host the back-end servers that enable the App to function. Your company or employer has its own privacy and other policies that also apply to your use of the App and Exchange. Zix is not responsible for the privacy practices of your company or other third parties.
- with our customers in connection with us processing your information on their behalf, including to respond to your questions, fulfill your requests, and otherwise comply with applicable law.
- to the extent that we determine it is reasonably necessary or legally required in order for us to respond to lawful requests by public authorities (including to meet national security or law enforcement requirements), subpoenas, court orders, warrants, or other legal process.
- when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to a government request.
- to enable a third party partner or independent reseller to contact you to facilitate the renewal, support or purchase of Zix products and services.
- with credit card authorization processors, third-party financial institutions and related organizations for billing and payment purposes so that they can verify the credit card numbers, process the credit card payment transaction, and prevent fraud or misuse of credit card facilities.

- with your consent or where disclosure is necessary in order to complete a transaction to which you have consented.
- as otherwise described in this Policy.

Zix does not generally disclose personal information about you to any third parties for commercial purposes and does not sell personal information as the term “sell” is traditionally understood. However, to the extent the California Consumer Privacy Act (“CCPA”) is interpreted to include advertising technology activities such as those disclosed below in the Section entitled “Analytics and Advertising” as a “sale,” Zix will comply with applicable law as to such activity. For more information about how to opt-out of sale of personal information, see the Section below entitled “California Resident Rights.”

We use testimonials from our customers, with their express consent, in order to show our customers and potential customers how Zix services have benefited others. To request removal of your information from the testimonials on our Site, contact us at privacy@zixcorp.com. In some cases, we may not be able to remove your information, in which case we will let you know if we are unable to do so and why.

Without limiting the foregoing, Zix shares with certain business partners, advertisers, and other third parties certain aggregated or de-identified data that does not identify you, , and email metadata (such as domains of senders and recipients), for various purposes, including marketing, except as prohibited by applicable law.

Analytics and Advertising

To analyze traffic to our Sites (excluding zixmessagecenter.com and zixmessagecentre.com), Zix uses various web analytics services, which independently set and access their own tracking technologies (including cookies, web beacons, and embedded scripts) and collect or have access to information about you.

In addition, Zix works with network advertisers and ad agencies to serve our advertisements on other web sites, within third party applications, and across the Internet, and to provide us with information regarding the effectiveness of our advertisements. For example, if you clicked on a Zix advertisement that led you to one of our corporate sites, our service provider(s) and we can often determine which Zix advertisement you clicked on and where you were viewing the advertisement. However, Zix’s advertising providers do not receive information regarding your use of the ZixMessage Center or your Greenview Data or Erado accounts, such as any URL you access within the message center or email

message content you view.

We also target advertisements based on your IP address and your web browsing activity on non-Zix websites. Zix's advertising providers also store cookies and other tracking technologies on your device. You can visit www.networkadvertising.org/managing/opt_out.asp, which provides information regarding this practice by Network Advertising Initiative ("NAI") members, including the opt-out procedures of NAI members. If you are visiting this site from the European Union, you can opt-out of certain interest-based ads by visiting www.youronlinechoices.eu. Please note this does not opt you out of being served ads. You will continue to receive generic ads. Zix does not control the information collection, use, or sharing practices of third party analytics providers or advertisers. Some of these parties collect your information when you visit the Sites, Apps, Services, or other online websites and services. We are not responsible for effectiveness of, or compliance with, any third-parties' opt-out options or programs or the accuracy of their statements regarding their programs.

The Zix Companies have always considered our advertising technology partners to be Service Providers. However, regulators may interpret newer data protection laws such as the CCPA as characterizing certain kinds of digital advertising activities as "sales." In such an event, Zix will comply with applicable laws in connection with its use of such advertising technology services on its Sites, Apps, or Services.

Social Features

Some of our Sites offer publicly accessible blogs or community forums. You should be aware that any information you provide in these areas can be read, collected, and used by others who access them. To request removal of your information from our blog or community forum, contact us at privacy@zixcorp.com. In some cases, we may not be able to remove your information, in which case we will let you know if we are unable to do so and why. The blog or community forums include certain social features (also known as third-party widgets), which permit interactions that you initiate between the blog or community forums and a third party web site or service. Social features include enabling you to "like" or "share" our content on other web sites or services, such as Facebook, Google+, Twitter, or LinkedIn. If you use social features, Zix receives or has access to certain information about you and your use of the social features. These social features collect your IP address and which page you are visiting on the blog or community forum,

and they set a cookie to enable the social feature to function properly. Social features are either hosted by a third party or hosted directly by us. The information we collect or receive in connection with social features is subject to this Policy. The information collected and stored by the provider of the social features remains subject to the that third party's privacy practices, including whether the third party continues to share information with us, the types of information shared, your choices with regard to what is visible to others on that third party web site or service and whether your information can be deleted from the third party site.

Google API Services

In connection with certain services that it provides, Zix uses Google API Services as part of an authentication and authorization framework to request access to Google user data. The Google user data we request through the Google API Services includes email addresses and basic profile information, and Zix uses such Google user data to verify user email addresses and manage the provisioning of administrator status on its domains. Any Google user data Zix collects through Google API Services is only used for such purposes and deleted after such use.

Links and Online Tracking By Third Parties

The Site contains links to Web sites controlled by third parties. We have no control over the practices of the third party Web sites to which we link. Those Web sites automatically collect information about your visit to their site and use their own tracking technology (such as cookies, web beacons, or embedded scripts). Those Web sites are subject to the privacy policies of the third parties that control those Web sites, and not the Zix Privacy Policy. We encourage you to check the privacy policies of these Web sites before using them or disclosing any information to them. In addition, such third-party services are subject to the terms and conditions and privacy policies applicable to those services.

These include the following:

- Google services privacy: <https://policies.google.com/privacy?hl=en-GB>
<https://security.google.com/settings/security/permissions>

YouTube API Services

In connection with certain services that it provides (including its Information Archiving Services), Zix uses YouTube API Services. You are responsible for configuring applicable third-party platforms or systems to transmit Customer Data to the Archive Service. You are responsible for obtaining access approval from each individual end user. Third-party email, social media, and other communication services are not offered, controlled or provided by Zix, Zix is not responsible for how a third party transmits, accesses, processes, stores, uses or provides data to Zix. Data that you send on removable media to Zix for import into the Archive Service may be subject to import fees. In addition, such third-party services are subject to the terms and conditions and privacy policies applicable to those services.

- YouTube terms and conditions: <https://www.youtube.com/t/terms>

Your Ability to Manage Your Zix Company Account Information

You have the ability to set or change your ZixMail PassPhrase and encryption codes, ZixMessage Center PassPhrase, Greenview Data, Total Defense, or Erado account password at any time. For credentials managed by DeliverySlip, you can set or change your password at any time. If you are authenticating with an alternate identity provider, such as Microsoft Office 365, please refer to the identity providers regarding changing passwords. If you forget or would like to change your ZixMessage Center PassPhrase, you can create a new or ZixMessage Center PassPhrase by registering again.

You can request deletion or deactivation of any of your Zix Company accounts by sending an email to privacy@zixcorp.com. Please see the "Data Storage" section of this Policy to read about data storage after your account has been deleted. Please note that it takes up to 30 days for your deletion or deactivation request to come into effect.

Subject to certain exceptions, upon request and provided you provide us sufficient information to confirm your identity, we will provide you the information that you have

submitted to us through your Zix Company account(s) for the purpose of enabling you to correct, amend, or delete any inaccuracies. You can make this request to us via email at privacy@zixcorp.com or visit the Site for online help at www.zixcorp.com/support/contact-support or through other online privacy request forms that Zix makes available. If we are not able to provide the information that you are requesting within 30 days of receipt of your request, we will provide you a timeline for providing the requested information. If we deny access to your information, we will explain why access was denied and give you contact information for further inquiries regarding the denial of access. If you are unhappy with our answers you can write to our Chief Privacy Officer, who can also be reached at privacy@zixcorp.com.

If you no longer wish to receive marketing emails from Zix, you can opt-out by (1) following the instructions provided in the emails, as applicable; (2) sending an email to support@zixcorp.com; or (3) visiting the Site at www.zixcorp.com/support/contact-support.

Data subjects in Europe, and California consumers, have additional rights as set forth in the sections entitled "European Privacy Rights" and "California Privacy Rights", respectively, below.

Security

Zix takes reasonable precautions, including the maintenance of reasonable physical, electronic, and procedural safeguards, to help protect your information from loss, misuse, and unauthorized or illegal access, disclosure, alteration, modification, use or destruction. Zix has implemented reasonable security measures to help protect your email address and the Zix service passwords associated with your email address from unauthorized access or disclosure, alteration, unlawful destruction or accidental loss. When appropriate, Zix uses industry-standard encryption to protect certain data (e.g., credit card numbers) during transmission. The servers on which we store your information are kept in an environment that is controlled and monitored 24 hours per day, 7 days per week. Although Zix uses reasonable efforts to help protect your information, transmission via the Internet, Wi-Fi or mobile network is not completely secure and Zix cannot guarantee the security of your information. In particular, it remains your responsibility:

- To protect against unauthorized access to your use of the Sites and Services.

- To ensure no one else uses the Sites or Services while your machine is logged on to the Sites or Services (including by logging on to your machine through a mobile, Wi-Fi or shared access connection you are using).
- To log off or exit from the Sites and Services when not using them.
- To keep your password or other access information secret and all of your account details secure. Your Zix Company Service passwords and log in details are personal to you and should not be given to anyone else or used to provide shared access, for example, over a network.
- To maintain good Internet security. For example if your email account is compromised, this could allow access to your account with us. If your email account is compromised it could be used to ask us to reset a password and gain access to your account with us.

If you think that any of your accounts has been compromised you should change your account credentials with us, and in particular make sure any compromised account (even one from another service) does not allow access to your account with us. Never use the same passwords for different accounts (among the Zix Company Services or with respect to other unrelated services). You should also tell us as soon as you can so that we can try to help you keep your account secure and if necessary warn anyone else who could be affected.

Data Storage

Most account information (including email addresses, public keys, names, and mailing addresses, but excluding credit card information used for payment to Zix) is stored on multiple disk storage systems at our data centers in the United States or the United Kingdom or on servers in Canada, Singapore, and Amsterdam. This means that we redundantly store data on more than one server in one of those locations. We also store email messages on servers outside the United States and the United Kingdom including on servers in Canada, Singapore, and Amsterdam.

Zix stores only the salted hash of a Zix service password. This means that we don't hold your Zix service password itself but rather a unique encrypted version of it. ZixMessage Center email messages that you send or receive via Zix services will ordinarily expire from our disk storage systems based on the expiration time set by the sender at the time the email was sent (1 to 365 days from the day the email message was sent). If you request deletion of your Zix service account, that account will be deactivated and your email address and information will be removed from our user registration database associated

with that Zix service within 30 days, subject to any need we have to hold onto the data for longer to meet any legal, auditing or regulatory requirements and subject to any commitments we have given to third parties – for example your employer if your employer paid for your Zix Company Service account. You can also request deletion of all your Zix Company Service accounts. If we do delete any of your accounts, those accounts will be reinitiated if another email is sent to you using a Zix Company Service. Email header information maintained for purposes of transaction logging, and user account information maintained for disaster recovery purposes, will be held longer than the content of email messages, as described above, in order to provide Zix Company Services, and support, including technical support and business continuity, to our customers.

If you use advanced threat protection services, including ZixProtect and SpamStopsHere, there will be particular points in time when the content of email messages and attachments (including non-spam messages) will not be encrypted, including but not limited to during spooling for delivery and on the way to quarantine. Further, if you choose to use the manual review option, the content of those emails and attachments will be stored in unencrypted form for purposes of manual review.

Guidelines Regarding Children

Zix's Site, and Zix Company products and Services, are not designed for or directed to children under the age of 16, and Zix does not knowingly collect personal information as defined by the Children's Online Privacy Protection Act ("COPPA") or personal information as defined under the CCPA from anyone under the age of 16. If you are under the age of 16, please do not provide personal information of any kind whatsoever and please do not use Zix products and services or participate in Zix's surveys, contests, events, and other promotions.

Your California Privacy Rights

Shine the Light Customer Rights

When California customers provide personal information as defined by California's "Shine the Light" to a business, they have the right to request certain disclosures if that business shares the personal information (as narrowly defined under the Shine the Light law) with third parties or affiliates for the third parties' or affiliates' direct marketing purposes. Once per calendar year the customer has the right to request that the business provide a list of companies with which it shares the personal information for the third parties' or affiliates' direct marketing purposes, and a list of the categories of personal information that the business shares. As stated in this Policy, we do not share personal information as defined under the Shine the Light law with third parties or affiliates for those third parties' or affiliates' direct marketing purposes. California customers can request further information about our compliance with this law by e-mailing privacy@zixcorp.com or contacting us by mail at 2711 N. Haskell Avenue, Suite 2200, LB 36, Dallas, Texas 75204-2960, USA. Please note that we are only required to respond to one request per customer each year, and we are not required to respond to requests made by means other than through this e-mail address.

California Consumer Rights Under the CCPA

If you are a California resident and a consumer customer of Zix, which in most cases means you are a customer of Total Defense, you have the right effective January 1, 2020, to request access to personal information we have collected about you, and to request other disclosures regarding the categories of personal information we have disclosed about you for business purposes or commercial purposes and regarding the categories of personal information we have sold about you, over the last 12 months. You will also have the right effective January 1, 2020, to request that we delete personal information we hold about you if we collected the information directly from you. The Zix Companies, including Zix and AppRiver, generally provide services to business customers, not individual consumers. If you represent a business, you do not have rights to request access to our deletion of your information pursuant to the CCPA.

To exercise your access or deletion rights as a California resident consumer customer

email us at privacy@totaldefense.com, call us at (855) 221-9691 or contact us through our online privacy request form.

Effective January 1, 2020, to the extent Zix sells your personal information as the term "sell" is defined under CCPA, you have the right to opt-out of sales of your personal information to third parties at any time. Zix does not sell personal information as the term "sell" is traditionally understood. However, to the extent the CCPA is interpreted to include advertising technology activities such as those disclosed in the "Analytics and Advertising" section of our policy as a "sale," Zix will comply with applicable law as to such activity. Please click the button below if you wish to opt-out of the sale of your personal information.

Do Not Sell My Personal Information

As of the posting of this updated privacy policy, certain provisions of the CCPA are still in flux and may change. Zix reserves the right to revise the sections of this policy that are impacted by those changes until such time as the regulations are finalized. Given the potential changes in the law, the rights available to California residents may change at any time.

European Privacy Rights

If you are a data subject in Europe, you have the right to access, rectify, or erase any personal data we have collected about you. You also have the right to data portability and the right to restrict or object to our processing of personal data we have collected about you. In addition, you have the right to ask us not to process your personal data (or provide it to third parties to process) for marketing purposes or purposes materially different than for which it was originally collected or subsequently authorized by you. You have the right to withdraw your consent at any time for any data processing we do based on consent you have provided to us.

To exercise any of these rights, contact us as set forth in the section entitled "Privacy Policy Questions, Suggestions and Complaints" below and specify which right you intend to exercise. We will respond to your request within 30 days. We sometimes require additional information from you to allow us to confirm your identity. Please note that we store information as necessary to fulfil the purposes for which it was collected, and continue to retain and use the information even after a data subject request for purposes of our legitimate interests, including as necessary to comply with our legal obligations, resolve disputes, prevent fraud, and enforce our agreements.

If your information has been processed by us on behalf of one of our customers and you wish to exercise any rights you have with such information, please inquire with our customer directly. If you wish to make your request directly to Zix, please provide the name of the Zix customer on whose behalf Zix processes your information. We will refer your request to that customer, and will support them to the extent required by applicable law in responding to your request.

If you have any issues with our compliance, you have the right to lodge a complaint with a European supervisory authority.

Data Controller

EU data protection law makes a distinction between organizations that process personal data for their own purposes (known as "controllers") and organizations that process personal data on behalf of other organizations (known as "processors"). In limited circumstances, Zix (located at the address set forth in the section entitled "Purpose of this Policy" above) operates as a controller, such as in connection with data collected from non-subscribers who browse its Site and when Zix Company Services involves a direct to consumer relationship. However, Zix generally operates as a processor on behalf of its customers that use the Zix services. The customers are the data controllers and determine the purposes for which and the manner in which personal data are to be processed by Zix. Please visit the applicable customer's privacy policy for information about their privacy practices. Any questions that you have relating to such personal data and your rights under data protection law should therefore be directed to the customer as the controller, not to Zix.

Moreover, Zix has partnerships with resellers who offer Zix Services directly to consumers. The resellers are controllers of the personal data they collect while offering and selling Zix

Services to consumers. Please direct any questions you may have regarding personal data collected or processed by resellers of Zix Services to the reseller, not to Zix.

Lawful Basis for Processing

Data protection laws in Europe require a “lawful basis” for processing personal data. When we operate as a controller, our lawful bases include where: (a) you have given consent to the processing for one or more specific purposes; (b) processing is necessary for the performance of a contract with you; (c) processing is necessary for compliance with a legal obligation; or (d) processing is necessary for the purposes of the legitimate interests pursued by us or a third party, and your interests and fundamental rights and freedoms do not override those interests. Our legitimate interests include direct marketing and fraud prevention, among other things.

Privacy Shield

We are based in the U.S. and the information we collect is governed by U.S. law. If you are accessing the Site or the Zix services from outside of the U.S., please be aware that information collected through the Site or the Zix services are transferred to, processed, stored, and used in the U.S. and other jurisdictions. Data protection laws in the U.S. and other jurisdictions are different from those of your country of residence. Your use of the Site or Zix Services therefore constitutes your consent to the transfer to and from, processing, usage, sharing, and storage of your information in the U.S. and other jurisdictions as set forth in this Policy. If your data is collected in Europe, the United Kingdom or Switzerland, we will transfer your personal data subject to appropriate or suitable safeguards, such as the Privacy Shield Framework discussed below.

The Zix Companies participate in the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from the European Union, the United Kingdom and Switzerland to the U.S. These Zix Companies have certified to the Department of Commerce that they adhere to the Privacy Shield Principles of notice, choice, accountability for onward transfer, security,

data integrity and purpose limitation, access, and recourse, enforcement and liability. For purposes of this section, Zix refers to the following U.S. legal entities: Zix Corporation, ZixCorp Systems, Inc., ZixCorp Global Inc., Greenview Data, Inc., CM2.COM Inc. dba Erado, AppRiver, LLC, and Total Defense, Inc.

In accordance with our obligations under the Privacy Shield, and subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission, we hereby affirm our commitment to subject to the Privacy Shield Principles all personal data transferred from the European Union, the United Kingdom and Switzerland in reliance on the Privacy Shield. This means that, in addition to our other obligations under the Privacy Shield Principles, we shall be liable to you for any third party agent to which we transfer your personal data and that processes such personal data in a manner that violates the Privacy Shield Principles, unless we can demonstrate that we are not responsible for the resulting damages.

For inquiries or complaints regarding our compliance with Privacy Shield, please send us an email or letter at the address specified in the “Privacy Policy questions, suggestions and complaints” section below. If we are unable to resolve your complaint directly, you have the right to submit your complaint at no cost to you to JAMS at <https://www.jamsadr.com/eu-us-privacy-shield>. In the event there are residual complaints that have not been resolved by JAMS, or any other means, you have the right to seek a non-monetary remedy through binding arbitration to be provided to you in accordance with the Privacy Shield Principles.

To learn more about the Privacy Shield Framework, and to view the Zix Companies’ certifications, please visit <http://www.privacyshield.gov>. A list of companies certified under the Privacy Shield Framework is available at the following link: <https://www.privacyshield.gov/list>.

Certain of the Zix Companies are registered with the United Kingdom Information Commissioner’s Office. The Zix registration number is Z304946X, and the AppRiver number is ZA545976. You can view Zix’s registration on the **UK ICO website**.

Notification of Changes to this Policy

We update this privacy policy to reflect changes to our information practices. If we make any material changes we will notify you by email (sent to the e-mail address specified in your account) or by means of a notice on this Site (if you do not have a Zix Company

Services account) prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.

Privacy Policy Questions, Suggestions and Complaints

If you have questions, concerns or suggestions about this Policy or Zix's privacy practices, please contact us:

Company
ZIX CORP
AppRiver
Total Defense

DeliverySlip

Email
privacy@zixcorp.com
privacy@appriver.com
support@totaldefense.com
privacy@totaldefense.com
privacyofficer@deliveryslip.com

By Mail:
2711 N. Haskell Ave
Suite 2200, LB 36
Dallas, Texas
75204-2960, USA
(Attn: Compliance Officer)

By Phone:
+1 (214) 370-2200

Email Encryption

Email Threat Protection

Information Archiving

Backup and Recovery

Email Message Privacy

Secure File Share

Microsoft 365

Partners

Global Partner Program

Become a Partner

Find a Partner

Partner Portal

Solutions

Modernize the Workplace

Mitigate Compliance Risk

Protect Business Communications

Enhance Business Productivity

Industry

Financial Services

Healthcare

Information Technology

Manufacturing

Support

Phenomenal Care

Support Portal

Company

About Zix

Leadership

Careers

In the News

Contact Us

- [Legal Center](#)
- [Privacy & Security Center](#)
- [ESG](#)
- [Do Not Sell My Information](#)
- [Cookie Settings](#)
- [Accessibility](#)

©1999-2022 Zix Corporation. All rights reserved. This site and Zix marks are protected by copyright and trademark laws under U.S. and international law.

DATA PROCESSING AMENDMENT

Acceptance of your applicable terms of service (e.g., the applicable standard Terms and Conditions (www.zix.com/terms) ("Underlying Agreement"), incorporates the terms of this Data Protection Amendment ("DPA") into the Underlying Agreement by reference. If there is any conflict between a provision in this DPA and a provision in the Underlying Agreement, this DPA will control.

You acknowledge and agree that the ZixCorp Systems, Inc. subsidiary or affiliate that provides the applicable service ("Company"), will process personal information during or in connection with your use of the Subscription Services. "Personal Information" means information relating to identified or identifiable natural persons, or that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to, directly or indirectly, a particular individual, consumer, data subject, or household, or is defined as "personally identifiable information," "personal information," "personal data," or similar term under applicable data protection law. Company operates as a data processor in providing the Subscription Services to you. You are the data controller and you determine the purposes for which and the manner in which any personal data are, or are to be, processed by Company. For purposes of the California Consumer Privacy Act of 2018, California Civil Code § 1798.100 *et seq.* ("California Consumer Privacy Act" or "CCPA") you are a Business and Company is a Service Provider. Company processes the personal data on your behalf and according to your instructions as set forth in the Agreement. Company shall not: (a) sell the Personal Information; (b) retain, use, or disclose the Personal Information for any purpose other than for the specific purpose of performing the Subscription Services; (c) retain, use, or disclose the Personal Information for a commercial purpose other than providing the Subscription Services; or (d) retain, use, or disclose the Personal Information outside of the direct business relationship between Company and Customer. Company certifies that it understands these restrictions and will comply with them.

Company requires, and you hereby warrant and represent, that any personal data you submit to Company during or in connection with your use of the Subscription Services, has not been collected, stored, and transferred to Company in violation of any law, regulation, or contractual obligation applicable to you. You shall have sole responsibility for the accuracy, quality, and legality of the personal data and the means by which you acquired the personal data.

To the extent Customer's use of the Subscription Services or the Subscription Materials involves personal data originating outside of the United States, Customer (1) acknowledges and consents to the transfer of such personal data outside of its country of origin; (2) shall ensure that it has provided any required notice to, and obtained any required consent(s) from, individuals for the processing of their personal data by Company and for the transfer of their personal data outside of its country of origin; (3) shall comply with all privacy and data protection laws applicable to such personal data; and (4) shall indemnify and hold Company and its affiliates harmless from and against any and all claims, causes of action, liabilities, penalties, costs or expenses incurred by Company or any affiliate thereof as result of your breach or violation of the provisions of this Section 4. Company self-certifies to and complies with the EU-US Privacy Shield Framework, as administered by the US Department of Commerce, and will maintain its self-certification to and compliance with the EU-US Privacy Shield Framework with respect to the processing of personal data that is transferred from the European Economic Area to the United States for the Subscription Services.

To the extent your use of the Subscription Services involves the processing by Company of the personal data of data subjects located in the European Union or otherwise subject to Regulation (EU) 2016/679, the General Data Protection Regulation, together with any additional implementation legislation, rules or regulations that are issued by applicable supervisory authorities ("GDPR"), the following provisions apply. Words and phrases shall, to the greatest extent possible, have the meanings given to them in the GDPR.

- I. Company shall process personal data on your behalf, according to your instructions, and in accordance with the GDPR requirements directly applicable to Company's provision of the Subscription Services. The following specifications apply ("Specifications"):
 - a. The subject matter of the processing is the performance of the Subscription Services to you pursuant to the Agreement. Company may process the personal data for the following purposes: (1) processing in accordance with the Agreement; (2) processing initiated by your end users in their use of the Subscription Services; and (3) processing to comply with other documented reasonable instructions provided by you (e.g., via email) where such instructions are consistent with the terms of the Agreement.
 - b. The duration of the processing is for the duration of the Agreement except where otherwise required by applicable law, as required by a legal obligation or for Company to protect its rights or those of a third party, or as required for Company to continue processing personal data based on a legitimate interest.
 - c. The categories of data subjects about whom Company processes personal data are determined and controlled by you, in your sole discretion, which may include, but are not limited to, your end users.

- d. The types of personal data that Company processes are determined and controlled by you, in your sole discretion, and may include, but are not limited to the categories of data identified in Exhibit A.
2. Company shall process the personal data only on documented instructions from you and in accordance with the Specifications above, unless required to do otherwise by applicable law to which Company is subject; in such a case, Company shall inform you of that legal requirement before processing personal data, unless that law prohibits such disclosure on important grounds of public interest. The Agreement constitutes your complete and final documented instructions, and any additional or alternate instructions must be agreed upon separately.
3. Company shall, to the extent legally permitted, promptly notify you if Company receives a request from a data subject to exercise the data subject's right of access, right to rectification, restriction of processing, erasure ("right to be forgotten"), data portability, objection to processing, or right not to be subject to automated individual decision making ("Data Subject Request"). Taking into account the nature of the processing, Company shall assist you, insofar as is possible, in the fulfilment of your obligation to respond to a Data Subject Request. In addition, to the extent you, in your use of the Subscription Services, do not have the ability to address a Data Subject Request, Company shall upon your written request provide commercially reasonable efforts to assist you in responding to such Data Subject Request, to the extent Company is legally permitted to do so and the response to such Data Subject Request is required under applicable laws. To the extent legally permitted, you shall be responsible for any costs arising from Company's provision of such assistance. Please note that Company may not be able to fulfill a Data Subject Request where to do so would violate laws applicable to Company, would interfere with Company's ability to meet legal obligations or protect its rights or those of a third party, or would prevent Company from continuing to process personal data where it has a legitimate interest in doing so.
4. You acknowledge and agree that Company may retain third party service provider subprocessors during or in connection with your use of the Subscription Services. Company shall enter into a written agreement with each subprocessor containing data protection obligations not less protective than those in the Agreement with respect to the protection of your personal data to the extent applicable to the services provided by the third party service provider. Company shall ensure that persons authorized to carry out processing have committed themselves to confidentiality or are under the appropriate statutory obligation of confidentiality. You hereby provide Company with general written authorization to engage such subprocessors in connection with this Agreement. Company shall be liable for the acts and omissions of its subprocessors to the same extent Company would be liable if performing the services of each subprocessor directly under the terms of the Agreement.
5. Upon your written request, Company shall provide you with reasonable cooperation and assistance as needed and appropriate to fulfil your obligations under the GDPR to carry out a data protection impact assessment related to your use of the Subscription Services, to the extent you do not otherwise have access to the relevant information, and to the extent such information is available to Company. Company shall provide reasonable assistance to you in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating the data protection impact assessment, to the extent required under the GDPR.

Exhibit A to Data Processing Addendum

Categories of data

The personal data transferred may include but is not limited to the categories of data set out below.

Personal Data

- Name
- Email Address
- Data present in email contents
- Email Metadata, including IP address

Sensitive Personal Data (depending on what is included in email contents)

- Race
- Ethnic origin
- Political opinion
- Religious beliefs
- Physical/mental health
- Sexual orientation
- Criminal offences (or proceedings which involve them).