Privacy Policy

1. INTRODUCTION

This privacy policy will let you know all the security policies and measures taken by **Xecurify Inc (DBA miniOrange Security Software Private Limited)** to protect the personally Identifiable Information(Mostly Referred for Google User Data present on GSuite / Google Apps Marketplace). Our primary goal is to have a secure connection between people and technology. miniOrange believes in creating products and services that are secure, resilient and assured. We have implemented various security guards to protect all personal information in accordance with industry standards.

2. MINIORANGE ROLES AND RESPONSIBILITIES

Please note that this privacy policy is applied to our customers/clients/partners who are using miniOrange Products to provide Cloud and In house based Solutions. These solutions will particularly require your personal information to provide you with appropriate security.
Each of our customers is aware of the information they provide to miniOrange; they have control and rights to restrict miniorange about the use of personal information. This content will include information such as first name, last name, phone number, email address, department you work or any such information that the customer chooses to submit.
miniOrange processes this data as a Service provider and when a customer chooses to process this information. miniOrange will not be responsible for the privacy of the customer's personal information that is not described in this privacy policy.

3. DATA COLLECTION

This section applies to how miniOrange collects personal information from the Gsuite (Google Apps) in the following ways -
The Google User data is requested by the user or the administrator responsible for using the miniOrange services for Authentication purposes.

1. miniOrange collects personal information of the user or administrator. This information includes
    a. Email
    b. First Name
    c. Last Name

d. And Other Contact information if applicable.

miniOrange does not store your password at the servers so your passwords cannot be retrieved by anyone but you.
This information helps us to categorize the question, track potential problems and trends and customize our support responses to better serve you.

2. We also collect your device specific information (e.g. mobile and desktop) from you in order to provide the Services. Device-specific information includes attributes (e.g. hardware model, operating system, web browser version, as well as unique device identifiers), connection information (e.g. name of your mobile operator or ISP, browser type, language and time zone, and mobile phone number); and device locations (e.g. internet protocol addresses and Wi-Fi). This information is particularly useful for providing you the services.

4. PROCESSING OF THE REQUESTED DATA /GOOGLE USER DATA

Enroll in the miniOrange Application

The users can be enrolled into miniOrange App in following ways:

1. By visiting account registration Page : In this, the admin shares the registration URL with the end-users, by visiting which they can create an account in miniOrange.
2. User Account Creation through Admin: In this, the admin creates accounts for individual users to enroll them into miniOrange. The account credentials are then shared with the users. The same can be achieved by creating a CSV in required format andD uploading the users in Bulk.
3. Using Provisioning: miniOrange provides the option to admin where he can configure provisioning with G Suite using OAuth Scopes and Directory SDK to import users from G Suite into miniOrange. [Email, First & Last Name, Phone no. are imported].

In all three methods of enrolling users, the admin has full control over the data and the enroll process.

It also allows IT administrators to analyze the employee's behavior towards enterprise data. On detection of a possible breach, it instantly sends an alert email message to notify higher business authorities. miniOrange also renders the program to enforce access control standards at the macro level on the idea of the IP address

Data Access:- To provide access control which helps organizations to specify data control policies on the idea of IP address through which G Suite content is often accessed. It imposes conditional policies on customer's Google for business accounts and creates a virtual secure environment.

Who is requesting Google user data?

miniOrange processes this data as a Service provider. The data is requested by the user or the administrator who is using our services for configuration and authentication purposes. The admin has full control over the requested data.

Use of the Google Apps Data/Information

Why does miniOrange collect the information?

miniOrange collects the requested information solely to provide the requested services to the users. Below are the purposes for which the data is requested and processed.

a. To Enroll you in the services -[mentioned above]
b. To provide the Security Services requested by the user.
c. To operate and improve our services.
d. To provide the response to user requests with the appropriate information.
e. To provide an additional layer of security by keeping out untrusted organizations.

All the data requested and processed only after the consent is provided by the administrator for the concerned Google Workspace account at the time of the Account Creation with miniOrange.

How does miniOrange use the Information?

- miniOrange app uses your IP Restriction policy to provide or deny access to the users based on trusted IP Addresses.
- For the IP Restriction to work, the Admin must create a policy specifying permitted IP addresses which allows the access to the google apps. Admin solely has the access and is responsible for providing the data to miniOrange to make the application work.
- Application will block the access if a user tries to access from a non trusted or non whitelisted IP address , thus keeping an eye out for unauthorized activity on your accounts.

How the Information is Stored and Protected?

All data for users such as the email address and First and Last name is provided only by the administrator [Directly or via a Sync].

While storing the user's data, the admin has the option of creating and sharing the password for the user's account in miniOrange or the user can set the password for his miniOrange account. The stored information is used only for authentication and related services.

All of the user's data is stored securely on RDS servers managed in AWS and are accessible only from miniOrange private EC2 instances.

So, the user's use a different password from their Google Account password to login via miniOrange App.

The user's data is used at the time of authentication as mentioned in the above section, to provide an additional layer of security on top of the user authentication. We are not storing your Google Account password, instead a new password is created for the user. miniOrange will only keep your personal information for as long as we reasonably require and in any event only for as long as the data protection legislation allows.

miniOrange provides security against any unauthorized domain, allowing one particular domain for the service.

SECURITY PRACTISES ON COLLECTED DATA

miniOrange maintains and uses reasonable administrative, organizational, technical and physical safeguards to protect your information from loss, destruction, misuse, unauthorized access or disclosure as required by applicable law. These technologies help ensure that your data is safe, secure, and only available to you and to those you provided authorized access (e.g., your users, admins,etc).

- miniOrange takes several steps to secure data. For all queries, retrievals, and bulk updates, the miniOrange service returns or updates only validated data. All miniOrange system responses to a request are subject to any access restrictions in place for that customer and their miniOrange registered users. This user/customer relationship is revalidated on every request to ensure that only authorized users within the customer's subdomain view the data.
- Our state-of-the-art encryption technology protects customer data both at rest and in transit to the user's browser, leaving no weak spots for attackers. miniOrange encrypted DB instances provide an additional layer of data protection by securing your data from unauthorized access to the underlying storage. We use Amazon RDS encryption to increase data protection of applications deployed in the cloud, and to fulfill compliance requirements for data-at-rest encryption.
- miniOrange uses Amazon KMS (key management service) to encrypt data symmetrically. This uses cryptographic keys for our applications and is a useful technique for data encryption. miniOrange uses different versions of RSA, DSA, TRIPLE-DES, AES and HMAC as required.
- All access to miniOrange uses the https protocol. Customers are assigned their own domains, sub-domains, and cookies.
- miniOrange uses strong encryption to secure sensitive customer data such as unique SAML keys that are created for authentication. We also store and encrypt credentials that users submit for secure browser applications (apps), configured within their SSO environment.
- miniOrange does not implement any proprietary encryption. Customer data encryption is performed at the application layer. The use of application level encryption protects sensitive data, even in the event of partial compromise.
- miniOrange encrypts the customer confidential data in the database. The encryption is performed using symmetric encryption 256-bit AES with exclusive keys. Customer exclusive symmetric keys ensure data segregation.

- Amazon Web Services (AWS) - provides the infrastructure that hosts miniOrange's Identity-as-a-Service platform. AWS SOC 2 report is available here: https://aws.amazon.com/artifact/
- For more information on security practises: https://idp.miniorange.com/security-practices-at-miniorange/

5. INFORMATION COLLECTED ON BEHALF OF THE CUSTOMERS USING OUR SERVICES

miniOrange collects information under the direction of its customers and has no direct relationship with the individual Users/employees whose personal data it processes. miniOrange works with its customers to help them provide notice to their employees concerning the purpose for which personal information is collected. We collect information for our customers. If you are an employee of one of our customers and would no longer like to use miniOrange's service, please contact your Employer directly. miniOrange may transfer Personal Information to companies that help us provide our service. Transfers to subsequent third parties are covered by the provisions in this Policy regarding notice and choice and the service agreements with our Customers. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data should direct their query to their Employer. If the Employer/miniOrange's Customer requests that miniOrange remove the data, we will respond to their request within 30 business days. miniOrange will retain Personal Information we process on behalf of our customers for as long as needed to provide services to our customer. miniOrange will retain and use this Personal Information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

6. COMPLIANCE WITH LIMITED USE REQUIREMENTS

miniOrange App's use of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements.- i.e

This App will not allow any unauthorized person to read this data unless they have their admin rights.

We take steps to protect your personal information from unauthorized access and against unlawful processing , accidental loss , destruction and damage or mentioned in point 4.

This app will not use google user data for any third party services or any advertising partners and market research purposes

The App will not allow humans to read this data unless we have your affirmative agreement for specific messages, doing so is necessary for security purposes such as investigating abuse, to comply with applicable law, or for the App's internal operations and even then only when the data have been aggregated and anonymized.

7. YOUR CHOICES ON INFORMATION

In the above section, we described how we collect and use your data. Below we have described how you can opt-out and modify settings related to our processing of your personal data.

You can change your information at any time by editing your account, or by closing your account. You can also ask us for additional information we may have about your account. You have a right to (1) access, modify, correct, or delete your personal information controlled by miniOrange regarding your account, and (2) close your account. You can also contact us for any account information which is not readily accessible to you.

8. CHANGES IN THE POLICY

We will notify you when we change this Privacy Policy. We may change this Privacy Policy from time to time. If we make significant changes in the way we treat your personal information, or to the Privacy Policy, we will provide notice by posting an announcement on the Website or sending an email prior to the change becoming effective.

9. CONTACT

If you would like to contact us with questions or concerns about our privacy policies and practices, you may contact us via any of the following methods:

Email us at: info@xecurify.com

For any queries: https://faq.miniorange.com/

Or call us at: **+1 978 658 9387**

Or you can fill form with your question/concern: https://www.miniorange.com/contact