SECURITY

Red e App

Last updated on February 3, 2017

RED E APP SECURITY POLICIES AND YOUR PRIVACY

We understand that keeping data secure is critical to everyone. Organizations and users across the world entrust Red e App with their data, and we make it a priority to take their security and privacy concerns seriously.

We have a comprehensive Privacy Policy that provides a very transparent view of our approach to privacy and the protection of your information. You can view our Privacy Policy here. It is important to note that if you are using Red e App in your workplace or on an organization issued device, your organization will likely have its own policies in place regarding your communications and use of Red e App. In addition to reviewing our policies, you should also check with your organization or network administrator to see what policies they have in place.

If you have additional questions regarding our data protection and privacy policies, please contact us at support@redeapp.com. Additionally, if you believe you have discovered a security vulnerability, we request that you to contact us right away. We will investigate all legitimate reports and take appropriate action when necessary.

KEEPING DATA SAFE AT RED E APP

The purpose of this Security Policy is to be transparent about our security infrastructure and business practices in order to reassure you that your data is safe. So, whether you are a representative of an organization or an end user of Red e App, here is everything you need to know about the protection of your data.

SECURITY

Secure Physical Location. Our servers are located in Amazon's AWS Data Centers. A detailed explanation of AWS' security procedures can be found at https://aws.amazon.com/security/ and https://aws.amazon.com/compliance.

Traffic Data Encryption. Red e App uses 256-bit AES, supports TLS 1.2 for all of your messages and uses the ECDHE RSA Key Exchange Algorithm. We monitor the security community's output closely and work promptly to upgrade Red e App Services to respond to new vulnerabilities as they are discovered.

External Security Audits. We contract with a respected external security firm who performs regular audits of Red e App to verify that our security practices are sound and to monitor Red e App Service in light of new vulnerabilities discovered by the security research community.

Multi-Step Authentication. Private Red e App networks can only be accessed with a valid username and password and a unique organization ID key, preventing unauthorized users from accessing private networks and an organization's data.

Revoke Access: Remove Resources, Files, and Messages. Upon dismissal or disassociation with an organization, an employee or organization affiliate user's access to an organization's network and related content and messaging capabilities can be removed and restricted.

PHI and HIPAA Compliant Messaging. Red e App meets all required criteria of HIPAA regulations ensuring the protection of personal health information and related data.

AVAILABILITY

We realize that our end users, and the organizations they represent, rely heavily on continuous and uninterrupted access to the Red e App application in order to conduct business. As a result, it is our commitment to you that we are constantly focused on ensuring Red e App is reliable and consistently available for your continued use. The Red e App platform is designed to withstand availability issues and unscheduled downtime through continuous application uptime and customer support monitoring, and by practicing server and operational redundancy standards and employing disaster recovery measures.

CONFIDENTIALITY

Your privacy and the confidentiality of your organization's data is very important to us, and it is our priority to protect it. We regard the information you share within your organization as private and confidential to your organization. In order to provide your organization, employees, and affiliates with the ultimate user experience and a fully functional application, it is necessary for Red e App's technical employees to maintain sufficient system permissions to access system source code and indirectly your organization's content. As a result, we have implemented strict controls over our employees' access to data and we are committed to limiting access to your organization's data solely for the purposes of maintaining and improving the Red e App platform. We require all of our employees and contractors to acknowledge and agree to our policies regarding user data privacy and protection.