Changefirst Security Statement

Thousands of users have entrusted Changefirst with their data, and we make it a priority to take our users' security and privacy concerns seriously. We strive to ensure that user data is kept securely, and that we collect only as much personal data as is required to provide our services to users in an efficient and effective manner.

Changefirst uses some of the most advanced technology for Internet security that is commercially available today. This Security Statement is aimed at being transparent about our security infrastructure and practices, to help reassure you that your data is appropriately protected.

Application and User Security

- **SSL/TLS Encryption:** e-change uses SSL/TLS protocol during transmission over public networks such as the internet. This ensures that user data in transit is safe, secure, and available only to intended recipients.

- **User Authentication:** User data on our database is logically segregated by account-based access rules. User accounts have unique usernames and passwords that must be entered each time a user logs on. e-change issues a session cookie (see our Cookie Policy for more information) only to record encrypted authentication information for the duration of a specific session. The session cookie does not include the password of the user.

- **User Passwords:** User application passwords have minimum complexity requirements. Passwords must meet the following guidelines:

    - be at least eight characters and no more than 20 characters in length
    - contain at least one number [0-9]
    - contain at least one lowercase letter [a-z]
    - contain at least one uppercase letter [A-Z]
    - contain at least one of these special characters: ! @ # $ % ^ & * ( ) + ?

- **Data Encryption:** Certain sensitive user data such as account passwords are stored in an encrypted format.

- **Data Portability:** e-change enables you to export your data from our system in a variety of formats so that you can back it up, or use it with other applications.

- **Privacy:** We have a comprehensive Privacy Policy that provides a very transparent view of how we handle your data, including how we use your data, who we share it with, and how long we retain it.

Physical Security

- **Data Center:** Our information systems infrastructure (servers, networking equipment, etc.) is located at a third party SSAE 16/SOC 2 audited data centre. Our data centres are unmarked to help maintain a low profile and these physical security measures are audited by an independent company.

- **Data Center Security:** Our data centres are staffed and monitored 24/7. Access is secured by security guards, visitors logs, and two-factor authentication entry requirements such as proximity access cards and biometric authentication.

- **Environmental Controls:** Our data centres are maintained at controlled temperatures and humidity ranges which are continuously monitored for variations. Smoke, floor water and fire detection and response systems are in place.

- **Location:** Our data centres are situated away from areas of geographic instability or those prone to

natural disasters. All user data is stored on servers located within the United Kingdom.

Availability

- **Connectivity:** Fully redundant IP network connections with multiple independent connections to a range of Tier 1 Internet access providers.

- **Power:** Our data centres are equipped with uninterruptible power supplies (UPS) to mitigate the risk of short-term utility power failures and fluctuations. The UPS power subsystems are N+1 redundant with instantaneous failover in the event of a primary UPS failure. The UPS systems are inspected at least twice annually. Data centre facilities are equipped with diesel generators to mitigate the risk of long-term utility power failures and fluctuations. Generators are regularly tested and maintained to provide assurance of appropriate operability in the event of an emergency. Data centre personnel are on duty 24 hours a day, 7 days a week.

- **Uptime:** Continuous uptime monitoring, with immediate escalation to Changefirst staff for any downtime.

Network Security

- **Uptime:** Continuous uptime monitoring, with immediate escalation to Changefirst staff for any downtime.

- **Third Party Scans:** Weekly security scans are performed by Qualys.

- **Testing:** System functionality and design changes are verified in an isolated test "sandbox" environment and subject to functional and security testing prior to deployment to active production systems.

- **Firewall:** External access to firewall is restricted to all ports except 443 (https).

- **Patching:** Latest security patches are applied to all operating system and application files to mitigate newly discovered vulnerabilities.

- **Access Control:** Secure VPN, multifactor authentication, and role-based access is enforced for systems management by authorized engineering staff.

- **Logging and Auditing:** Central logging systems capture and archive all internal systems access including any failed authentication attempts.

Storage Security

- **Backup Frequency:** Backups occur 4 hourly and daily to a centralized onsite backup system. Backups are retained for a two week period.

Organizational & Administrative Security

- **Employee Screening:** We perform routine background screening on all employees.

- **Training:** We provide security and technology use training for employees.

- **Service Providers:** We screen our service providers and bind them under contract to appropriate confidentiality obligations if they deal with any user data.

- **Access:** Access controls to sensitive data in our databases, systems and environments are set on a need-to-know / least privilege necessary basis.

- **Audit Logging:** We maintain and monitor audit logs on our services and systems.

- **Information Security Policies:** We maintain internal information security policies, including incident

response plans, and regularly review and update them.

Software Development Practices

- **Stack:** We code in Java and C# and run on SQL Server 2008 and Windows 2008 Server.

- **Coding Practices:** Our engineers use best practices and industry-standard secure coding guidelines to ensure secure coding.

Handling of Security Breaches

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if Changefirst learns of a security breach, we will notify affected clients so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under various state and federal laws and regulation, as well as any industry rules or standards that we adhere to. Notification procedures include providing email notices or posting a notice on our website if a breach occurs.

Your Responsibilities

Keeping your data secure also depends on you ensuring that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems, to keep any data you download to your own computer away from prying eyes.

Custom Requests

Due to the number of customers that use our service, specific security questions or custom security forms can only be addressed for customers purchasing a certain volume of user accounts within a Changefirst Enterprise subscription. If your company has a large number of potential or existing users and is interested in exploring such arrangements, please contact info@changefirst.com.

Last updated: 2nd December 2015