Data Security Statement - CMNTY Corporation (CMNTY)

Last modified: May 26, 2020

1. DEFINITIONS

Please note that, unless we define a term in this Data Security Statement, all capitalized terms used in this Data Security Statement have the same meaning as in our Terms of Use. So, please make sure that you have read and understand our General Terms and Conditions.

2. SCOPE

The purpose of this Security Statement is to communicate to CLIENT the security measurements CMNTY has in place to protect the data and privacy of Users. This document may not be shared with any other party than CLIENT without the written permission of CMNTY.

3. PARTIES RESPONSIBLE

Two parties are identified, each with their own responsibilities towards maintaining an acceptable security level towards (sensitive) User data.

1. CMNTY, who applies security measurements to the infrastructure and supplies CLIENT with tools to secure the Platform.
2. CLIENT, who configures and operates the Platform.

4. ORGANISATIONAL MEASURES

1. **Accreditations**
   CMNTY is ISO 27001:2013 certified and regularly performs internal audits on its working processes. We are audited once a year by the independent auditing institute named BSI Group.

2. **Compliance**
   CMNTY is GDPR and CCPA compliant. Currently CMNTY is in the process of becoming HIPAA compliant.

3. **Incident management**
   CMNTY's internal working procedure covers the process of detecting, reporting and communicating any security incidents. CLIENT is informed about any threats, risks, timing, impact and, when possible, solutions ultimately within 72 hours after detection of the security incident.

4. **Responsible person(s)**
   Storage and protection of electronic data on CMNTY's servers is monitored continuously by CMNTY's CTO and his team.

5. **Documentation**
   All data collected using the Platform is protected in accordance with CMNTY's General Terms and Conditions, Service Level Agreement and Privacy Policy.

6. **Human resources**
   Upon selection of potential employees, CMNTY carefully screens employment references and obtains evidence of stated academic and professional qualifications, followed by independent identity checks. CMNTY employees are obliged to conform with a non-disclosure clause upon signing their employment contract. A thorough check-out procedure is performed on all employees upon resignation or dismissal.

7. **Third-party**
   To reduce the risk of any security threats to the lowest possible minimum, CMNTY demands ISO 27001:2013 compliance from all infrastructure partners. A mandatory non-disclosure clause is included in all contracts with all third parties.

5. IT SECURITY MEASURES

1. **Acceptable use of hardware and internal systems**
   Acceptable use of internal systems and hardware is covered by CMNTY's *acceptable use policy* and each individual employment contract signed by all CMNTY employees.

2. **Development and testing**
   Software development is only performed on local devices. Staging servers are physically separated from production servers. Testing and deployment is performed by authorised personnel only. CMNTY carries out functional, usability, design and vulnerability tests all of which are performed on separate servers.

3. **Encryption**
   All communication between User and the Software is encrypted via **SSL/HTTPS**. CMNTY uses **4096 bit** encryption keys. Passwords are always stored as hashes.

4. **Data storage and backups**
   All CLIENT data is stored only on ISO 27001:2013-compliant servers. All information is labelled in accordance with CMNTY's internal working procedures. All data is backed up daily (every 24 hour) on a separate server. Backup data is encrypted and stored for a period of 30 days and automatically deleted afterwards.

5. **Business continuity**
   In order to ensure business continuity we strive to maintain the following parameters:
   a. Recovery Time Objective (RTO) is 12 hours according to P1 incidents as described in our SLA.
   b. Recovery Point Objective (RPO) is 24 hours according to daily backups as described in our SLA.

6. **Network security**
   CMNTY's office network connection is protected using a firewall, all incoming ports are blocked. CMNTY's server stack consists of a network of servers that do not allow incoming internet traffic except when accessed via a secure VPN connection. There are only proxy servers reachable on web ports 80 and 443 and these servers are physically separated from servers containing CLIENT data. Only authorised personnel has access to the VPN server using personal keys. Only a subset of our (development) employees can access servers with CLIENT data. Access to these servers is further restricted using a personal SSH keypair. All of CMNTY's Platform servers have alert packages installed to detect break-in attempts or other suspicious behaviour. In case such attempts or behaviour is detected, CMNTY will be warned through automated emails. Office guests are provided with a separate WiFi connection.

7. **Anti-virus and spyware protection**
   CMNTY office devices and systems are protected with anti-spyware and anti-virus tools.

8. **Penetration tests**
   CMNTY performs an application penetration every month or on request. The test is performed by the CTO and action to increase security is taken if the reports indicate to do so. Due to the intensity of this test, CMNTY is entitled to charge a fee to CLIENT when this test is made on request. A copy of the latest application penetration test can be sent to CLIENT on request.

6. PLATFORM SECURITY MEASURES

1. **Passwords**
   CMNTY supplies CLIENT with the following options in regard to password security;
   a. Character requirements
   b. Minimum password length
   c. Password expiration
   d. Prevent password reuse
   e. Allow change of password only once every 24 hours.

2. **2FA**
   2FA can be turned on, on a per role basis. Either using SMS, Google Authenticator or -e-mail.

3. **Sessions**
   CMNTY supplies CLIENT with the following options in regards of sessions:
   a. Duration of a session
   b. Log off on closing the browser

4. **Rate limiting**
   CMNTY has applied rate limiting to the following pages in Platform;
   a. Reset password / change password
   b. Sign off
   c. 2FA
   d. API authentication

   Additionally CLIENT can configure the rate limit for the login page and the lockdown time.

5. **IP Access**
   CLIENT is capable of limiting access to Platform by using a predefined list of IP-Addresses.

6. **reCAPTCHA**
   reCAPTCHA can be turned on for the registration page when working with open or protected platforms.

7. **Headers**
   CMNTY sets the following response headers:
   a. Referrer-Policy: strict-origin-when-cross-origin
   b. X-Content-Type-Options: nosniff
   c. X-XSS-Protection: 1, mode=block
   d. Strict-Transport-Security: max-age=15768000

   Additionally CMNTY provides CLIENT with the option to turn the following headers on;
   e. X-Frame-Options: SAMEORIGIN
   f. Content-Security-Policy: <>

   A header test can be conducted, free of charge, by using the following website: https://securityheaders.io/

8. **SSL**
   Platform is protected by an SSL certificate with 4096 bits encryption key. We do not support weak connections,

   A SSL test can be conducted, free of charge, by using the following website: https://www.ssllabs.com/ssltest/analyze.html

9. **Anti-Virus**
   All servers are equipped with anti-virus software, scanning all uploads for malicious files and removing them if encountered.

7. PHYSICAL SECURITY MEASURES

1. **Physical allocation**
   CMNTY servers are stored off CMNTY premise in a secured environment of Amazon AWS. Sensitive hard copy files are stored in our CMNTY office in a secured room, in locked cabinets. The building is secured with a key and alarm code both of which provided to a restricted number of employees for the purposes of security assurance. All office laptops are encrypted and password-protected. Additional policies like the *Device Configuration Policy*, *Password Policy* and *Remote Access Policy* apply to all employees.

2. **Use of removable devices for data storage**
   CMNTY does not store any personal and/or sensitive data in removable USB memory sticks. Any personal and/or sensitive data collected via the Platform are stored in secured servers and, occasionally, on encrypted and password-protected office laptops. All office laptops are equipped with file vault to encrypt all laptop data as per our *Device Configuration Policy.*

3. **Re-use of hardware**
   Any data-containing equipment is reset to default and double-checked for any data or software traces afterwards. In case of hardware re-use, after the reset, the new employee is provided with a personal, password-protected account.

8. DATA COLLECTION STATEMENT & DISCLAIMER

CMNTY, acting as a processor, receives and processes personal data on behalf of CLIENT. CMNTY will never act as a controller, only CLIENT will be considered a controller.

The type of personal data collected via CMNTY Platform will depend on the content that is uploaded by CLIENT and its Users. CLIENT is ultimately responsible to provide its Users with all information mandatory by law, such as the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;. Users shall be encouraged by CMNTY to contact CLIENT with any questions regarding the collection and use of their personal data.

CMNTY does not accept any liability in respect of any information on its CMNTY Platform supplied by CLIENT and/or Users.